CS 70 Midterm 2 Review

Mona Gupta, Peter Qian, Kevin Wu, Sung Roa Yoon, Alton Zheng

Eta Kappa Nu, Mu Chapter
University of California, Berkeley

March 31 2013

Summary: Polynomials

Property 1: A non-zero polynomial of degree d has at most d roots.

Summary: Polynomials

Property 1: A non-zero polynomial of degree d has at most d roots.

Example:
$x^3 + 2x^2 + 3 = 0$
↑ Degree 3, so maximum 3 roots
$x + 3x^2 + 4 = x^4$
↑ Degree 4, so maximum 4 roots

Summary: Polynomials

Property 1: A non-zero polynomial of degree d has at most d roots.

Example:
$x^3 + 2x^2 + 3 = 0$
↑ Degree 3, so maximum 3 roots
$x + 3x^2 + 4 = x^4$
↑ Degree 4, so maximum 4 roots

Property 2: Given $d + 1$ points $(x_1, y_1), (x_2, y_2), ..., (x_{d+1}, y_{d+1})$ with all the x_i distinct, there exists a unique polynomial $p(x)$ of degree at most d that passes through all the points.

Summary: Polynomials

Property 1: A non-zero polynomial of degree d has at most d roots.

Example:
$x^3 + 2x^2 + 3 = 0$
↑ Degree 3, so maximum 3 roots
$x + 3x^2 + 4 = x^4$
↑ Degree 4, so maximum 4 roots

Property 2: Given $d + 1$ points $(x_1, y_1), (x_2, y_2), ..., (x_{d+1}, y_{d+1})$ with all the x_i distinct, there exists a unique polynomial $p(x)$ of degree at most d that passes through all the points.

Example:
$(-1, 2), (0, 1), (2, 5)$
Degree of at most two!

Polynomial Generation

Find the polynomial that passes through the three points $(0,2),(-1,3),(1,1)$.

Polynomial Generation

Find the polynomial that passes through the three points $(0, 2), (-1, 3), (1, 1)$.

Solution 1: Linear Equations
$p(x) = a_2x^2 + a_1x + a_0$

$a_2(0)^2 + a_1(0) + a_0 = 2$
$a_2(-1)^2 + a_1(-1) + a_0 = 3$
$a_2(1)^2 + a_1(1) + a_0 = 1$
$\Rightarrow$
$a_0 = 2$
$a_2 - a_1 + a_0 = 3$
$a_2 + a_1 + a_0 = 1$

$a_0 = 2, a_2 = 0, a_1 = -1 \rightarrow p(x) = -x + 2$ □

Polynomial Generation

Find the polynomial that passes through the three points $(0, 2), (-1, 3), (1, 1)$.

Solution 2: Lagrange Interpolation

$f_1 = (x + 1)(x - 1)$

$\uparrow f_1 = \dfrac{(x + 1)(x - 1)}{(0 + 1)(0 - 1)}$

$\uparrow f_1 = 2\dfrac{(x + 1)(x - 1)}{(0 + 1)(0 - 1)} = -2x^2 + 2$

Polynomial Generation

Find the polynomial that passes through the three points $(0,2),(-1,3),(1,1)$.

Solution 2: Lagrange Interpolation

$$f_1 = (x+1)(x-1)$$

$$\uparrow f_1 = \frac{(x+1)(x-1)}{(0+1)(0-1)}$$

$$\uparrow f_1 = 2\frac{(x+1)(x-1)}{(0+1)(0-1)} = -2x^2+2$$

$$f_1 = 2\frac{(x+1)(x-1)}{(0+1)(0-1)} = -2x^2+2$$

$$f_2 = 3\frac{(x-0)(x-1)}{(-1-0)(-1-1)} = \frac{3}{2}x^2 - \frac{3}{2}x$$

$$f_3 = 1\frac{(x-0)(x+1)}{(1-0)(1+1)} = \frac{1}{2}x^2 + \frac{1}{2}x$$

$p(x) = f_1 + f_2 + f_3 = -x + 2$ □

Finite Fields

Polynomial coefficients and variables can only take on certain integer values. Denoted as $GF(q)$.

Finite Fields

Polynomial coefficients and variables can only take on certain integer values.
Denoted as $GF(q)$.

Both properties about polynomials hold if and only if q is prime! This is because the proofs use division, which is only guaranteed to be possible if q is prime.

Secret Sharing

If we want to share a message with n people such that k people or more can decode the message but less than k people learn nothing:
1) Create a polynomial $p(x)$ of degree $k-1$.
2) Let $p(0) =$ "secret".
3) Hand out $p(1), ..., p(n)$ to the n people.

- k or more people can decode the message.
- Any less and they learn nothing.

Functions and Finite Fields

How many distinct functions exist in GF(4)?

Functions and Finite Fields

How many distinct functions exist in GF(4)?

4 values for x.
4 choice for y for each x.
4 values of x, so we can generate a distinct function with 4 choices
$4^4 = 256$ □

Functions and Finite Fields

How many distinct functions exist in GF(4)?

4 values for x.
4 choice for y for each x.
4 values of x, so we can generate a distinct function with 4 choices
$4^4 = 256$ □

q^q functions exist in $GF(q)$!

Not enough points!

Find a degree 2 polynomial that passes through the points (1,1), (2,1).

Not enough points!

Find a degree 2 polynomial that passes through the points (1,1), (2,1).

Not enough points, so pick an arbitrary point. Let's pick (0,0).

$$
\begin{aligned}
f_1 &= \frac{0(x-1)(x-2)}{(0-1)(0-2)} = 0 \\
f_2 &= \frac{1(x-0)(x-2)}{(1-0)(1-2)} = -x^2 + 2x \\
f_3 &= \frac{0(x-0)(x-1)}{(2-0)(2-1)} = \frac{1}{2}x^2 - \frac{1}{2}x
\end{aligned}
$$

$$f_1 + f_2 + f_3 = -\frac{1}{2}x^2 + \frac{3}{2}x \quad \square$$

True/False

If a polynomial has degree 10 in $GF(51)$ the polynomial has at most 10 roots.

True/False

If a polynomial has degree 10 in $GF(51)$ the polynomial has at most 10 roots.

False! 51 is not prime, so none of the properties hold in $GF(51)$. □

True/False

There is a unique polynomial, $p(x)$ in $GF(7)$ of degree 1 such that $p(134) = 8$ and $p(15) = 36$.

True/False

There is a unique polynomial, $p(x)$ in $GF(7)$ of degree 1 such that $p(134) = 8$ and $p(15) = 36$.

False! In $GF(7)$, 134, 8, 15, and 36 are all equivalent to 1. Therefore, you are only given the point (1,1), which does not determine a unique degree one polynomial. □

Error Correcting Codes

Erasure Errors: If the message is n packets long and we want to recover from an erasure of at most k packets:
1) Create a degree $n-1$ polynomial $p(x)$.
2) Let the message be encoded in either the coefficients of $p(x)$ or the actual values.
3) Send $p(1), ..., p(n+k)$.

Error Correcting Codes

Erasure Errors: If the message is n packets long and we want to recover from an erasure of at most k packets:
1) Create a degree $n-1$ polynomial $p(x)$.
2) Let the message be encoded in either the coefficients of $p(x)$ or the actual values.
3) Send $p(1), ..., p(n+k)$.

General Errors: If the message is n packets long and we want to recover from k malicious errors:
1) Create a degree $n-1$ polynomial $p(x)$.
2) Let the message be encoded in either the coefficients of $p(x)$ or the actual values.
3) Send $p(1), ..., p(n+2k)$.

Generals and Nukes

The president wants to share the nuclear launch code, 5 characters long, between his 5 generals such that any 3 can uncover the original code. However, spies are meddling with the communication system so 2 packets have a chance to be deleted when he sends each general their code. Devise a system where he can be sure that his generals receive the right codes while retaining the secret's integrity.

Generals and Nukes

The president wants to share the nuclear launch code, 5 characters long, between his 5 generals such that any 3 can uncover the original code. However, spies are meddling with the communication system so 2 packets have a chance to be deleted when he sends each general their code. Devise a system where he can be sure that his generals receive the right codes while retaining the secret's integrity.

This problem tests two concepts: (1) Secret Sharing (2) Erasure Error Correction

Generals and Nukes

The president wants to share the nuclear launch code, 5 characters long, between his 5 generals such that any 3 can uncover the original code. However, spies are meddling with the communication system so 2 packets have a chance to be deleted when he sends each general their code. Devise a system where he can be sure that his generals receive the right codes while retaining the secret's integrity.

This problem tests two concepts: (1) Secret Sharing (2) Erasure Error Correction

Secret Sharing: 5 generals, 3 to uncover
1) $GF(q)$, where q is a large prime
2) $p(x) =$ degree 2 polynomial
3) Hand out $p(1), p(2), p(3), p(4), p(5)$

Generals and Nukes

The president wants to share the nuclear launch code, 5 characters long, between his 5 generals such that any 3 can uncover the original code. However, spies are meddling with the communication system so 2 packets have a chance to be deleted when he sends each general their code. Devise a system where he can be sure that his generals receive the right codes while retaining the secret's integrity.

This problem tests two concepts: (1) Secret Sharing (2) Erasure Error Correction

Secret Sharing: 5 generals, 3 to uncover
1) $GF(q)$, where q is a large prime
2) $p(x) =$ degree 2 polynomial
3) Hand out $p(1), p(2), p(3), p(4), p(5)$

Erasure Error Correction: 2 erasures
For each general:
1) Can still work in $GF(q)$
2) $r(x) =$ degree 0 polynomial
3) Let r(0) = the point we want to send
4) Send $r(1), r(2), r(3)$

Generals and Nukes

The president wants to share the nuclear launch code, 5 characters long, between his 5 generals such that any 3 can uncover the original code. However, spies are meddling with the communication system so 2 packets have a chance to be deleted when he sends each general their code. Devise a system where he can be sure that his generals receive the right codes while retaining the secret's integrity.

This problem tests two concepts: (1) Secret Sharing (2) Erasure Error Correction

Secret Sharing: 5 generals, 3 to uncover
1) $GF(q)$, where q is a large prime
2) $p(x) =$ degree 2 polynomial
3) Hand out $p(1), p(2), p(3), p(4), p(5)$

Erasure Error Correction: 2 erasures
For each general:
1) Can still work in $GF(q)$
2) $r(x) =$ degree 0 polynomial
3) Let r(0) = the point we want to send
4) Send $r(1), r(2), r(3)$
*Notice you're just sending the same point three times, does that make sense?

Example - Decoding General Errors

Alice is sending Bob a message consisting of '2' and '3'. There is a possibility of 1 malicious error from Eve. Working in GF(7).

(a) What should Alice send to Bob?

Example - Decoding General Errors

Alice is sending Bob a message consisting of '2' and '3'. There is a possibility of 1 malicious error from Eve. Working in GF(7).

(a) What should Alice send to Bob?

1) $p(x)$ is a degree one polynomial
2) $p(x) = 2x + 3$
3) $p(1), p(2), p(3), p(4)$
4) 5,7,9,11 $\rightarrow$ 5,0,2,4

Example - Decoding General Errors

Alice is sending Bob a message consisting of '2' and '3'. There is a possibility of 1 malicious error from Eve. Working in GF(7).

(a) What should Alice send to Bob?

1) $p(x)$ is a degree one polynomial
2) $p(x) = 2x + 3$
3) $p(1), p(2), p(3), p(4)$
4) 5,7,9,11 $\rightarrow$ 5,0,2,4

Eve changes it to: 5,0,0,4
(b) How does Bob decode the message?

Example - Decoding General Errors

Alice is sending Bob a message consisting of '2' and '3'. There is a possibility of 1 malicious error from Eve. Working in GF(7).

(a) What should Alice send to Bob?

1) $p(x)$ is a degree one polynomial
2) $p(x) = 2x + 3$
3) $p(1), p(2), p(3), p(4)$
4) 5,7,9,11 $\rightarrow$ 5,0,2,4

Eve changes it to: 5,0,0,4
(b) How does Bob decode the message?

$P(x) =$ correct polynomial of degree one
$E(x) = (x - e_1) = x + b_0$
$R(x) =$ polynomial that matches our points
$Q(x) = P(x)E(x) = a_2x^2 + a_1x + a_0$
$Q(x) = R(x)E(x)$

Example - Decoding General Errors

Values: 5,0,0,4

$Q(x) = R(x)E(x)$
$a_2x^2 + a_1x + a_0 = R(x)(x + b_0)$

Example - Decoding General Errors

Values: 5,0,0,4

$$Q(x) = R(x)E(x)$$
$$a_2x^2 + a_1x + a_0 = R(x)(x + b_0)$$

$$1a_2 + 1a_1 + 1a_0 = 5(1 + b_0)$$
$$4a_2 + 2a_1 + 1a_0 = 0(2 + b_0)$$
$$2a_2 + 3a_1 + 1a_0 = 0(3 + b_0)$$
$$2a_2 + 4a_1 + 1a_0 = 4(4 + b_0)$$

Example - Decoding General Errors

Values: 5,0,0,4

$Q(x) = R(x)E(x)$
$a_2x^2 + a_1x + a_0 = R(x)(x + b_0)$

$1a_2 + 1a_1 + 1a_0 = 5(1 + b_0)$
$4a_2 + 2a_1 + 1a_0 = 0(2 + b_0)$
$2a_2 + 3a_1 + 1a_0 = 0(3 + b_0)$
$2a_2 + 4a_1 + 1a_0 = 4(4 + b_0)$

$a_0 = 5, a_1 = 4, a_2 = 2, b_0 = 4$

Example - Decoding General Errors

Values: 5,0,0,4

$Q(x) = R(x)E(x)$
$a_2x^2 + a_1x + a_0 = R(x)(x + b_0)$

$1a_2 + 1a_1 + 1a_0 = 5(1 + b_0)$
$4a_2 + 2a_1 + 1a_0 = 0(2 + b_0)$
$2a_2 + 3a_1 + 1a_0 = 0(3 + b_0)$
$2a_2 + 4a_1 + 1a_0 = 4(4 + b_0)$

$a_0 = 5, a_1 = 4, a_2 = 2, b_0 = 4$
$Q(x) = 2x^2 + 4x + 5, E(x) = (x + 4)$

Example - Decoding General Errors

Values: 5,0,0,4

$Q(x) = R(x)E(x)$
$a_2x^2 + a_1x + a_0 = R(x)(x + b_0)$

$1a_2 + 1a_1 + 1a_0 = 5(1 + b_0)$
$4a_2 + 2a_1 + 1a_0 = 0(2 + b_0)$
$2a_2 + 3a_1 + 1a_0 = 0(3 + b_0)$
$2a_2 + 4a_1 + 1a_0 = 4(4 + b_0)$

$a_0 = 5, a_1 = 4, a_2 = 2, b_0 = 4$
$Q(x) = 2x^2 + 4x + 5, E(x) = (x + 4)$
$Q(x) = P(x)E(x) \Rightarrow Q(x)/E(x) = P(x)$

Example - Decoding General Errors

Values: 5,0,0,4

$Q(x) = R(x)E(x)$
$a_2x^2 + a_1x + a_0 = R(x)(x + b_0)$

$1a_2 + 1a_1 + 1a_0 = 5(1 + b_0)$
$4a_2 + 2a_1 + 1a_0 = 0(2 + b_0)$
$2a_2 + 3a_1 + 1a_0 = 0(3 + b_0)$
$2a_2 + 4a_1 + 1a_0 = 4(4 + b_0)$

$a_0 = 5, a_1 = 4, a_2 = 2, b_0 = 4$
$Q(x) = 2x^2 + 4x + 5, E(x) = (x + 4)$
$Q(x) = P(x)E(x) \Rightarrow Q(x)/E(x) = P(x)$

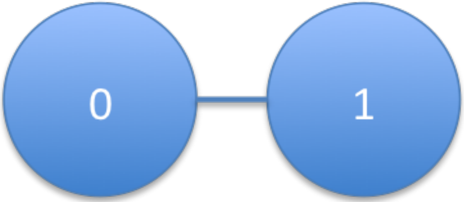
$$\frac{2x^2 + 4x + 5}{x + 4} = 2x + 3$$

Graphs

Eulerian Path: A path in a graph that uses each edge exactly once.
Hamiltonian Path: A path that goes through every vertex exactly once.
de Bruijn Sequence: 2^n-bit circular sequence such that every string of length n occurs as a contiguous substring of the sequence once.
de Bruijn Graph: G = (V,E) where V is the set of all n-1 bit strings, and the edges represent the transformation of a shift and addition of a new zero/one.
Hypercube: A graph in which all of the nodes are connected to other nodes who differ from them by 1 bit.

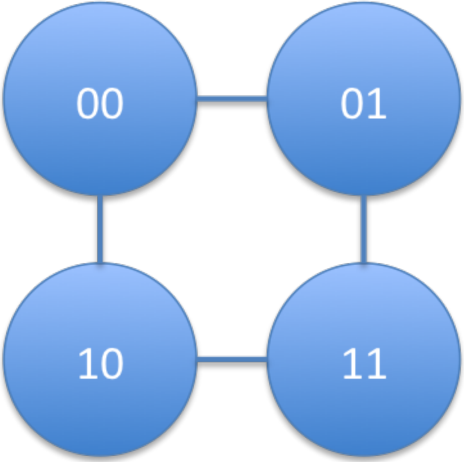
Visualizing 6D Hypercube

Let's try visualizing the hypercube in a way to comprehend up to 6 dimensions...
Here is the first dimension! (Simple, right?)
Note that there is one edge per node.



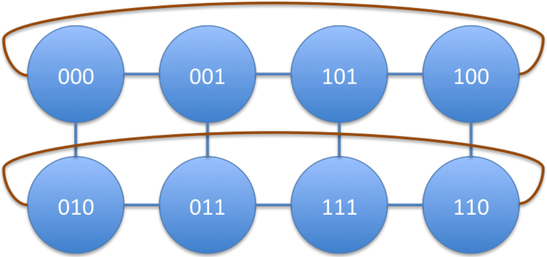
Visualizing 6D Hypercube

Here is the second dimension!
Note that there are two edges per node.



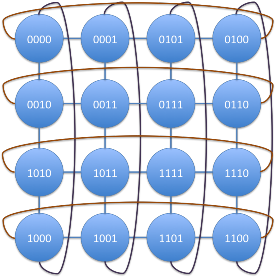
Visualizing 6D Hypercube

Here is the third dimension!
Note that there are three edges per node.
Here, instead of spreading to our conventional three dimensional space, let's visualize it in just a 2D space still, where we just have edge crossing over between left end and right end.



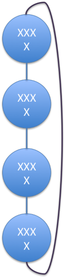
Visualizing 6D Hypercube

Here is the fourth dimension!
Note that there are four edges per node.
If you notice with the three dimension one, there is still one side on each node that is not used, right? So we can make use of that spot to spread to four dimensions in just 2D visual space.



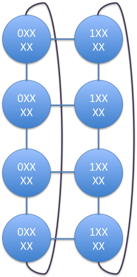
Visualizing 6D Hypercube

Now in the previous 2D virtual space, there is no more sides to make use of, right? Because of that, NOW we move onto 3D virtual space to try showing higher dimension. To go further, imagine that the 4D hypercube graph you saw earlier turned sideways. (Literally, move the paper 90 degrees).



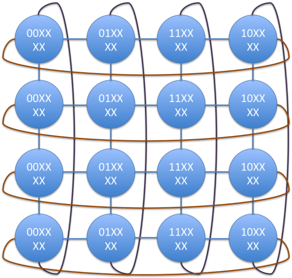
Visualizing 6D Hypercube

You can see how there are still two sides on each circle that haven't been used yet, right? We can make use of one of them to get us to visualize 5D hypercube!



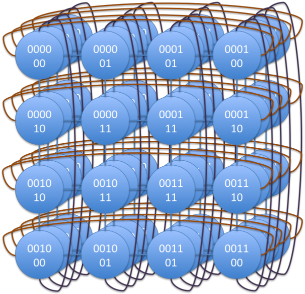
Visualizing 6D Hypercube

Now lastly, we make use of one more side left on the circle, and by filling that side, we have reached 6D hypercube.



Visualizing 6D Hypercube

That might have been a bit difficult, but I hope it wasn't too hard to understand? To put it in perspective of what we just visualized, here is how the full 6D hypercube would look to us at an angle!



Complete Graphs

Wikipedia: “A **complete** graph is an undirected graph in which every pair of distinct vertices is connected by a unique edge.”

(a) How many edges are in a complete graph with 100 nodes?

(b) Does an Eulerian path exist such a graph?

(c) Does an Eulerian cycle exist in such a graph?

(d) Does a Hamiltonian path exist in such a graph?

(e) Does a Hamiltonian cycle exist in such a graph?

Complete Graphs

Wikipedia: "A **complete** graph is an undirected graph in which every pair of distinct vertices is connected by a unique edge."

(a) How many edges are in a complete graph with 100 nodes? $\frac{100 \cdot 99}{2}$

(b) Does an Eulerian path exist such a graph?

(c) Does an Eulerian cycle exist in such a graph?

(d) Does a Hamiltonian path exist in such a graph?

(e) Does a Hamiltonian cycle exist in such a graph?

Complete Graphs

Wikipedia: "A **complete** graph is an undirected graph in which every pair of distinct vertices is connected by a unique edge."

(a) How many edges are in a complete graph with 100 nodes? $\frac{100 \cdot 99}{2}$

(b) Does an Eulerian path exist such a graph? No

(c) Does an Eulerian cycle exist in such a graph? No

(d) Does a Hamiltonian path exist in such a graph?

(e) Does a Hamiltonian cycle exist in such a graph?

Complete Graphs

Wikipedia: “A **complete** graph is an undirected graph in which every pair of distinct vertices is connected by a unique edge.”

(a) How many edges are in a complete graph with 100 nodes? $\frac{100 \cdot 99}{2}$

(b) Does an Eulerian path exist such a graph? No

(c) Does an Eulerian cycle exist in such a graph? No

(d) Does a Hamiltonian path exist in such a graph? Yes

(e) Does a Hamiltonian cycle exist in such a graph? Yes

Complete Graphs (cont.)

Now we generate a complete graph with 101 nodes. Then we remove 1 randomly chosen edge.

(a) Does an Eulerian path exist in this graph?

(b) Does an Eulerian cycle exist in this graph?

Complete Graphs (cont.)

Now we generate a complete graph with 101 nodes. Then we remove 1 randomly chosen edge.

(a) Does an Eulerian path exist in this graph? Yes

(b) Does an Eulerian cycle exist in this graph?

Complete Graphs (cont.)

Now we generate a complete graph with 101 nodes. Then we remove 1 randomly chosen edge.

(a) Does an Eulerian path exist in this graph? Yes

(b) Does an Eulerian cycle exist in this graph? No

(c) Now, what is the minimum number of edges you need to remove additionally to make this graph have an Eulerian cycle?

Complete Graphs (cont.)

Now we generate a complete graph with 101 nodes. Then we remove 1 randomly chosen edge.

(a) Does an Eulerian path exist in this graph? Yes

(b) Does an Eulerian cycle exist in this graph? No

(c) Now, what is the minimum number of edges you need to remove additionally to make this graph have an Eulerian cycle? 2

Hypercube Question

(a) If you have degree 4 hypercube and you remove one edge from it, does it have an Eulerian cycle?

Hypercube Question

(a) If you have degree 4 hypercube and you remove one edge from it, does it have an Eulerian cycle? No

(b) In that case, what is the minimum number of edges you need to remove additionally to make this graph have an Eulerian cycle?

Hypercube Question

(a) If you have degree 4 hypercube and you remove one edge from it, does it have an Eulerian cycle? No

(b) In that case, what is the minimum number of edges you need to remove additionally to make this graph have an Eulerian cycle? 3

Counting Words

(a) How many 7 letter words can be spelled with the 7 letters "abcdefg" without repeating any letter?

(b) How many 4 letter words can be spelled with the 7 letters "abcdefg" without repeating any letter?

(c) How many 4 letter words can you spell with 2 A's and 2 B's?

Counting Words

(a) How many 7 letter words can be spelled with the 7 letters “abcdefg” without repeating any letter? $7! = 5040$

(b) How many 4 letter words can be spelled with the 7 letters “abcdefg” without repeating any letter?

(c) How many 4 letter words can you spell with 2 A’s and 2 B’s?

Counting Words

(a) How many 7 letter words can be spelled with the 7 letters "abcdefg" without repeating any letter? $7! = 5040$

(b) How many 4 letter words can be spelled with the 7 letters "abcdefg" without repeating any letter? $\frac{7!}{3!} = 840$

(c) How many 4 letter words can you spell with 2 A's and 2 B's?

Counting Words

(a) How many 7 letter words can be spelled with the 7 letters "abcdefg" without repeating any letter? $7! = 5040$

(b) How many 4 letter words can be spelled with the 7 letters "abcdefg" without repeating any letter? $\frac{7!}{3!} = 840$

(c) How many 4 letter words can you spell with 2 A's and 2 B's? $\frac{4!}{2!}/2! = 6$

Two-Headed Monster

(a) When tossing 4 coins, what is the probability of getting exactly 2 heads?

(b) When tossing 4 coins, what is the probability of getting at least 2 heads?

Two-Headed Monster

(a) When tossing 4 coins, what is the probability of getting exactly 2 heads? $\frac{3}{8}$

(b) When tossing 4 coins, what is the probability of getting at least 2 heads?

Two-Headed Monster

(a) When tossing 4 coins, what is the probability of getting exactly 2 heads? $\frac{3}{8}$

(b) When tossing 4 coins, what is the probability of getting at least 2 heads? $\frac{11}{16}$

Playing with Dice

(a) When rolling 2 dice, what is the probability of snake eyes (i.e. two 1's)?

(b) When rolling 2 dice, what is the probability of getting one 1 and one 2?

(c) When rolling 4 dice, what is the probability of getting four 1's?

(d) When rolling 4 dice, what is the probability of getting two 1's and two 3's?

Playing with Dice

(a) When rolling 2 dice, what is the probability of snake eyes (i.e. two 1's)? $\frac{1}{36}$

(b) When rolling 2 dice, what is the probability of getting one 1 and one 2?

(c) When rolling 4 dice, what is the probability of getting four 1's?

(d) When rolling 4 dice, what is the probability of getting two 1's and two 3's?

Playing with Dice

(a) When rolling 2 dice, what is the probability of snake eyes (i.e. two 1's)? $\frac{1}{36}$

(b) When rolling 2 dice, what is the probability of getting one 1 and one 2? $\frac{1}{18}$

(c) When rolling 4 dice, what is the probability of getting four 1's?

(d) When rolling 4 dice, what is the probability of getting two 1's and two 3's?

Playing with Dice

(a) When rolling 2 dice, what is the probability of snake eyes (i.e. two 1's)? $\frac{1}{36}$

(b) When rolling 2 dice, what is the probability of getting one 1 and one 2? $\frac{1}{18}$

(c) When rolling 4 dice, what is the probability of getting four 1's? $\frac{1}{6^4} = \frac{1}{1296}$

(d) When rolling 4 dice, what is the probability of getting two 1's and two 3's?

Playing with Dice

(a) When rolling 2 dice, what is the probability of snake eyes (i.e. two 1's)? $\frac{1}{36}$

(b) When rolling 2 dice, what is the probability of getting one 1 and one 2? $\frac{1}{18}$

(c) When rolling 4 dice, what is the probability of getting four 1's? $\frac{1}{6^4} = \frac{1}{1296}$

(d) When rolling 4 dice, what is the probability of getting two 1's and two 3's?
$(\frac{1}{6^4}) \cdot 6 = \frac{1}{6^3} = \frac{1}{216}$

Bayesian Inference Basics

Let's say you are given Pr[A], $Pr[B|A]$, and $Pr[B|\overline{A}]$. How do you find $Pr[A|B]$?

Bayesian Inference Basics

Let's say you are given Pr[A], $Pr[B|A]$, and $Pr[B|\overline{A}]$. How do you find $Pr[A|B]$?

$$Pr[A|B] = \frac{Pr[A \cap B]}{Pr[B]} \tag{1}$$

$$Pr[B|A] = \frac{Pr[A \cap B]}{Pr[A]} \Rightarrow Pr[A \cap B] = \frac{Pr[B|A]}{Pr[A]} \tag{2}$$

$$Pr[B] = Pr[A \cap B] + Pr[\overline{A} \cap B] = Pr[B|A]Pr[A] + Pr[B|\overline{A}](1 - Pr[A]) \tag{3}$$

$$Pr[A|B] = \frac{Pr[B|A]Pr[A]}{Pr[B|A]Pr[A] + Pr[B|\overline{A}](1 - Pr[A])} \tag{4}$$

Line 2 refers to Baye's Rule and line 3 refers to the Total Probability Rule.

Am I Crazy?

Chris wants to know if he has bipolar disorder. Let C be the event that Chris has bipolar disorder. The incidence of bipolar disorder in the general population is 1%. He is really poor, so he asks his older brother Alex to make his diagnosis. If someone has bipolar disorder, Alex correctly identifies it 80% of the time, but if someone does not have bipolar disorder, Alex makes a false accusation of bipolar 30% of the time. Let A be the event that Alex diagnoses Chris of having bipolar disorder. Assume $Pr[C] = 0.01$.

Am I Crazy?

Chris wants to know if he has bipolar disorder. Let C be the event that Chris has bipolar disorder. The incidence of bipolar disorder in the general population is 1%. He is really poor, so he asks his older brother Alex to make his diagnosis. If someone has bipolar disorder, Alex correctly identifies it 80% of the time, but if someone does not have bipolar disorder, Alex makes a false accusation of bipolar 30% of the time. Let A be the event that Alex diagnoses Chris of having bipolar disorder. Assume $Pr[C] = 0.01$.

(a) Find $Pr[A|C]$

(b) Find $Pr[A]$

(c) Find $Pr[C|A]$ (The probability that Chris has bipolar disorder given that Alex diagnoses him with bipolar disorder).

(d) Let B be the event that Chris receives a correct diagnoses from Alex. Find $Pr[B]$

Am I Crazy?

Chris wants to know if he has bipolar disorder. Let C be the event that Chris has bipolar disorder. The incidence of bipolar disorder in the general population is 1%. He is really poor, so he asks his older brother Alex to make his diagnosis. If someone has bipolar disorder, Alex correctly identifies it 80% of the time, but if someone does not have bipolar disorder, Alex makes a false accusation of bipolar 30% of the time. Let A be the event that Alex diagnoses Chris of having bipolar disorder. Assume $Pr[C] = 0.01$.

(a) Find $Pr[A|C]$ 0.8 (Read this straight from problem statement)

(b) Find $Pr[A]$

(c) Find $Pr[C|A]$ (The probability that Chris has bipolar disorder given that Alex diagnoses him with bipolar disorder).

(d) Let B be the event that Chris receives a correct diagnoses from Alex. Find $Pr[B]$

Am I Crazy?

Chris wants to know if he has bipolar disorder. Let C be the event that Chris has bipolar disorder. The incidence of bipolar disorder in the general population is 1%. He is really poor, so he asks his older brother Alex to make his diagnosis. If someone has bipolar disorder, Alex correctly identifies it 80% of the time, but if someone does not have bipolar disorder, Alex makes a false accusation of bipolar 30% of the time. Let A be the event that Alex diagnoses Chris of having bipolar disorder. Assume $Pr[C] = 0.01$.

(a) Find $Pr[A|C]$ 0.8 (Read this straight from problem statement)

(b) Find $Pr[A] = Pr[A|C] \cdot Pr[C] + Pr[A|\bar{C}] \cdot Pr[\bar{C}]$
$= (0.8) \cdot (.01) + (0.3) \cdot (1 - .01) = 0.305$

(c) Find $Pr[C|A]$ (The probability that Chris has bipolar disorder given that Alex diagnoses him with bipolar disorder).

(d) Let B be the event that Chris receives a correct diagnoses from Alex. Find $Pr[B]$

Am I Crazy?

Chris wants to know if he has bipolar disorder. Let C be the event that Chris has bipolar disorder. The incidence of bipolar disorder in the general population is 1%. He is really poor, so he asks his older brother Alex to make his diagnosis. If someone has bipolar disorder, Alex correctly identifies it 80% of the time, but if someone does not have bipolar disorder, Alex makes a false accusation of bipolar 30% of the time. Let A be the event that Alex diagnoses Chris of having bipolar disorder. Assume $Pr[C] = 0.01$.

(a) Find $Pr[A|C]$ 0.8 (Read this straight from problem statement)

(b) Find $Pr[A] = Pr[A|C] \cdot Pr[C] + Pr[A|\bar{C}] \cdot Pr[\bar{C}]$
$= (0.8) \cdot (.01) + (0.3) \cdot (1 - .01) = 0.305$

(c) Find $Pr[C|A]$ (The probability that Chris has bipolar disorder given that Alex diagnoses him with bipolar disorder). $= \frac{Pr[A|C] \cdot Pr[C]}{Pr[A]} = \frac{0.8 \cdot 0.01}{0.305} = \frac{8}{305}$

(d) Let B be the event that Chris receives a correct diagnoses from Alex. Find $Pr[B]$

Am I Crazy?

Chris wants to know if he has bipolar disorder. Let C be the event that Chris has bipolar disorder. The incidence of bipolar disorder in the general population is 1%. He is really poor, so he asks his older brother Alex to make his diagnosis. If someone has bipolar disorder, Alex correctly identifies it 80% of the time, but if someone does not have bipolar disorder, Alex makes a false accusation of bipolar 30% of the time. Let A be the event that Alex diagnoses Chris of having bipolar disorder. Assume $Pr[C] = 0.01$.

(a) Find $Pr[A|C]$ 0.8 (Read this straight from problem statement)

(b) Find $Pr[A] = Pr[A|C] \cdot Pr[C] + Pr[A|\bar{C}] \cdot Pr[\bar{C}]$
$= (0.8) \cdot (.01) + (0.3) \cdot (1 - .01) = 0.305$

(c) Find $Pr[C|A]$ (The probability that Chris has bipolar disorder given that Alex diagnoses him with bipolar disorder). $= \frac{Pr[A|C] \cdot Pr[C]}{Pr[A]} = \frac{0.8 \cdot 0.01}{0.305} = \frac{8}{305}$

(d) Let B be the event that Chris receives a correct diagnoses from Alex. Find $Pr[B]$
$= Pr[A \cap C] + Pr[\bar{A} \cap \bar{C}]$
$= Pr[A|C] \cdot Pr[C] + Pr[\bar{A}|\bar{C}] \cdot Pr[\bar{C}] = 0.701$

Am I Crazy? (cont.)

(e) Let's generalize the answer to (d). Let D be the event that a psychologist diagnoses Chris as having bipolar disorder. $Pr[D|C] = p$ and $Pr[D|\neg C] = q$. Let $Pr[C] = s$. Let B' be the event that Chris receives a correct diagnosis from the psychologist.

Am I Crazy? (cont.)

(e) Let's generalize the answer to (d). Let D be the event that a psychologist diagnoses Chris as having bipolar disorder. $Pr[D|C] = p$ and $Pr[D|\neg C] = q$. Let $Pr[C] = s$. Let B' be the event that Chris receives a correct diagnosis from the psychologist.

   i Find $Pr[B']$.

   ii What is the effect of raising p? (Does this make intuitive sense?)

   iii What is the effect of raising q? (Does this make intuitive sense?)

   iv What is the effect of raising s? (Why is this the case?)

Am I Crazy? (cont.)

(e) Let's generalize the answer to (d). Let D be the event that a psychologist diagnoses Chris as having bipolar disorder. $Pr[D|C] = p$ and $Pr[D|\neg C] = q$. Let $Pr[C] = s$. Let B' be the event that Chris receives a correct diagnosis from the psychologist.

i Find $Pr[B']$. $sp + (1 - s)(1 - q)$

ii What is the effect of raising p? (Does this make intuitive sense?)

iii What is the effect of raising q? (Does this make intuitive sense?)

iv What is the effect of raising s? (Why is this the case?)

Am I Crazy? (cont.)

(e) Let's generalize the answer to (d). Let D be the event that a psychologist diagnoses Chris as having bipolar disorder. $Pr[D|C] = p$ and $Pr[D|\neg C] = q$. Let $Pr[C] = s$. Let B' be the event that Chris receives a correct diagnosis from the psychologist.

i Find $Pr[B']$. $sp + (1-s)(1-q)$

ii What is the effect of raising p? (Does this make intuitive sense?)
Increases accuracy of diagnosis

iii What is the effect of raising q? (Does this make intuitive sense?)

iv What is the effect of raising s? (Why is this the case?)

Am I Crazy? (cont.)

(e) Let's generalize the answer to (d). Let D be the event that a psychologist diagnoses Chris as having bipolar disorder. $Pr[D|C] = p$ and $Pr[D|\neg C] = q$. Let $Pr[C] = s$. Let B' be the event that Chris receives a correct diagnosis from the psychologist.

i Find $Pr[B']$. $sp + (1 - s)(1 - q)$

ii What is the effect of raising p? (Does this make intuitive sense?)
Increases accuracy of diagnosis

iii What is the effect of raising q? (Does this make intuitive sense?)
Decreases accuracy of diagnosis

iv What is the effect of raising s? (Why is this the case?)

Am I Crazy? (cont.)

(e) Let's generalize the answer to (d). Let D be the event that a psychologist diagnoses Chris as having bipolar disorder. $Pr[D|C] = p$ and $Pr[D|\neg C] = q$. Let $Pr[C] = s$. Let B' be the event that Chris receives a correct diagnosis from the psychologist.

i Find $Pr[B']$. $sp + (1 - s)(1 - q)$

ii What is the effect of raising p? (Does this make intuitive sense?)
Increases accuracy of diagnosis

iii What is the effect of raising q? (Does this make intuitive sense?)
Decreases accuracy of diagnosis

iv What is the effect of raising s? (Why is this the case?)
It depends...

Bayesian Inference

There are three indistinguishable boxes. One of them has 2 prize balls out of 10, another one has 4 prize balls out of 10, and the last one has 0 prize balls out of 10. The previous contestant chose from a random box and drew a prize ball out. What is the probability that he drew from the box with 2 prize balls given that he drew a prize ball?

Bayesian Inference

There are three indistinguishable boxes. One of them has 2 prize balls out of 10, another one has 4 prize balls out of 10, and the last one has 0 prize balls out of 10. The previous contestant chose from a random box and drew a prize ball out. What is the probability that he drew from the box with 2 prize balls given that he drew a prize ball?

Let A = event that the chosen box has 2 prizes.

Let B = event that the previous contestant got a prize ball.

$$\begin{aligned}
Pr[A] &= 1/3 \\
Pr[B|A] &= .2 \\
Pr[B|\neg A] &= .2 \\
Pr[A|B] &= \frac{Pr[B|A]Pr[A]}{Pr[B|A]Pr[A] + Pr[B|\neg A](1 - Pr[A])} \\
Pr[A|B] &= \frac{0.2 * 0.33}{0.2 * 0.33 + 0.2 * 0.67} \\
Pr[A|B] &= 0.33
\end{aligned}$$

More Bayesian Inference

Since the previous contestant just drew a prize ball, Now, there are 9 balls in that box, while the other boxes still have 10 balls. To get the best chance of obtaining a prize ball, should you select that box? Or try choosing from one of the other two boxes?

More Bayesian Inference

Since the previous contestant just drew a prize ball, Now, there are 9 balls in that box, while the other boxes still have 10 balls. To get the best chance of obtaining a prize ball, should you select that box? Or try choosing from one of the other two boxes?

First, you need to find the probability that the previous contestant chose the 4 prizes box.

Let C = event that the chosen box has 4 prizes.

Let B = event that the previous contestant got a prize ball.

$$
\begin{aligned}
Pr[C] &= 1/3 \\
Pr[B|C] &= .4 \\
Pr[B|\neg C] &= .1 \\
Pr[C|B] &= \frac{Pr[B|C]Pr[C]}{Pr[B|C]Pr[C] + Pr[B|\neg C](1 - Pr[C])} \\
Pr[C|B] &= \frac{0.4 * 0.33}{0.4 * 0.33 + 0.1 * 0.67} \\
Pr[C|B] &= 0.67
\end{aligned}
$$

More Bayesian Inference

Since the previous contestant just drew a prize ball, Now, there are 9 balls in that box, while the other boxes still have 10 balls. To get the best chance of obtaining a prize ball, should you select that box? Or try choosing from one of the other two boxes?

First, you need to find the probability that the previous contestant chose the 4 prizes box.
Let C = event that the chosen box has 4 prizes.
Let B = event that the previous contestant got a prize ball.

$$
\begin{aligned}
Pr[C] &= 1/3 \\
Pr[B|C] &= .4 \\
Pr[B|\neg C] &= .1 \\
Pr[C|B] &= \frac{Pr[B|C]Pr[C]}{Pr[B|C]Pr[C] + Pr[B|\neg C](1 - Pr[C])} \\
Pr[C|B] &= \frac{0.4 * 0.33}{0.4 * 0.33 + 0.1 * 0.67} \\
Pr[C|B] &= 0.67
\end{aligned}
$$

Or if you aren't silly like me, you could have just seen that the probability of it being 4 prizes given someone got a prize from there is just
$1 - Pr[\text{chosen box has 2 prizes}|\text{previous contestant got a prize}]$.

More Bayesian Inference (cont.)

Since the previous contestant just drew a prize ball, Now, there are 9 balls in that box, while the other boxes still have 10 balls. To get the best chance of obtaining a prize ball, should you select that box? Or try choosing from one of the other two boxes?

Now that you have that information, you can get the expected value of drawing from that box or drawing from one of the other boxes. Let's say the box that the last contestant drew from is called Q.

Let A = event that Q has 2 prizes.

Let B = event that the previous contestant got a prize.

Let C = event that Q has 4 prizes.

Let D = event that you win a prize by drawing from Q.

Let E = event that you win a prize by drawing from the other box.

$$Pr[D] = Pr[A|B] * 1/9 + Pr[C|B] * 3/9$$

$$Pr[D] = 0.26$$

$$Pr[E] = Pr[A|B] * 0.5 * 0.4 + Pr[C|B] * 0.5 * 0.2$$

$$Pr[E] = 0.13$$

Hashing Collision Probability

What is the largest number, m, of keys we can store before the probability of a collision reaches p?

Hashing Collision Probability

What is the largest number, m, of keys we can store before the probability of a collision reaches p?

How can we approach this problem?

Hashing Collision Probability

What is the largest number, m, of keys we can store before the probability of a collision reaches p?

How can we approach this problem?

Step 1: Express the problem formally.

Hashing Collision Probability

What is the largest number, m, of keys we can store before the probability of a collision reaches p?

How can we approach this problem?

Step 1: Express the problem formally.

Notice that $\Pr[\text{collision}] \leq p \equiv \Pr[\text{no collision}] \geq p$

It's much easier to express the probability of no collisions! Let's define this formally as:

Event A: Event that there are no collisions in a hash table with m items and n buckets.

Computing Pr[A]

Let's assume $m \leq n$. Otherwise, the probability that there are m non-colliding objects in n buckets is trivially zero.

Computing Pr[A]

Let's assume $m \leq n$. Otherwise, the probability that there are m non-colliding objects in n buckets is trivially zero.

We can think of this as a balls and bins problem! We simply want to throw m balls into n bins and calculate the probability that none of the balls collide.

Computing Pr[A]

Let's assume $m \leq n$. Otherwise, the probability that there are m non-colliding objects in n buckets is trivially zero.

We can think of this as a balls and bins problem! We simply want to throw m balls into n bins and calculate the probability that none of the balls collide.

$$\begin{aligned} Pr[A] =& Pr(\texttt{first ball doesn't collide}) \cdot Pr(\texttt{second ball doesn't collide}) \\ & \cdot \ldots \cdot Pr(\texttt{mth ball doesn't collide}) \\ =& \frac{n}{n} \cdot \frac{n-1}{n} \cdot \ldots \cdot \frac{n-(m-1)}{n} \end{aligned}$$

Here Comes the Math

Let's begin by taking the natural log of both sides.

Here Comes the Math

Let's begin by taking the natural log of both sides.

$$ln(Pr[A]) = ln(1 - \frac{1}{n}) + ln(1 - \frac{2}{n}) + ... + ln(1 - \frac{m-1}{n})$$

Here Comes the Math

Let's begin by taking the natural log of both sides.

$$ln(Pr[A]) = ln(1 - \frac{1}{n}) + ln(1 - \frac{2}{n}) + ... + ln(1 - \frac{m-1}{n})$$

Next, we're going to use the approximation $ln(1 - x) \approx -x$ if x is small.

Here Comes the Math

Let's begin by taking the natural log of both sides.

$$ln(Pr[A]) = ln(1 - \frac{1}{n}) + ln(1 - \frac{2}{n}) + ... + ln(1 - \frac{m-1}{n})$$

Next, we're going to use the approximation $ln(1-x) \approx -x$ if x is small. Rewriting our expression:

$$\begin{aligned} ln(Pr[A]) &\approx -\frac{1}{n} - \frac{2}{n} - ... - \frac{m-1}{n} \\ &= -\frac{1}{n}\sum_{i=1}^{m-1} i \\ &= -\frac{1}{n} \cdot \frac{m(m-1)}{2} \\ &\approx -\frac{m^2}{2n} \end{aligned}$$

Here Comes the Math

Let's begin by taking the natural log of both sides.

$$ln(Pr[A]) = ln(1 - \frac{1}{n}) + ln(1 - \frac{2}{n}) + ... + ln(1 - \frac{m-1}{n})$$

Next, we're going to use the approximation $ln(1 - x) \approx -x$ if x is small. Rewriting our expression:

$$\begin{aligned} ln(Pr[A]) &\approx -\frac{1}{n} - \frac{2}{n} - ... - \frac{m-1}{n} \\ &= -\frac{1}{n}\sum_{i=1}^{m-1} i \\ &= -\frac{1}{n} \cdot \frac{m(m-1)}{2} \\ &\approx -\frac{m^2}{2n} \end{aligned}$$

Let's do a little more math...

$$Pr[A] \approx e^{-\frac{m^2}{2n}}$$

Solving for m

So far we have:

$$Pr[A] \approx e^{-\frac{m^2}{2n}}$$

Solving for m

So far we have:

$$Pr[A] \approx e^{-\frac{m^2}{2n}}$$

This whole time, we've been trying to solve for Pr[A] $\geq$ p . So let's plug in and solve!

$$Pr[A] \approx e^{-\frac{m^2}{2n}} \geq p$$

$$-\frac{m^2}{2n} \geq ln(p)$$

$$m \leq \sqrt{2n \cdot ln(1/p)}$$

Bringing It All Together

(a) What assumptions/approximations are made in the derivation we just went through?

(b) If we halved the size of the hash table, how would the collision probability change? Recall $m \leq \sqrt{2n \cdot ln(1/p)}$.

Bringing It All Together

(a) What assumptions/approximations are made in the derivation we just went through?

1. Assumed $m \leq n$.
2. $ln(1-x) \approx -x$ when x is small
3. Assumed x is small
4. Approximated $\frac{m(m-1)}{2n} \approx \frac{m^2}{2n}$

(b) If we halved the size of the hash table, how would the collision probability change? Recall $m \leq \sqrt{2n \cdot ln(1/p)}$.

Bringing It All Together

(a) What assumptions/approximations are made in the derivation we just went through?

1. Assumed $m \leq n$.
2. $ln(1-x) \approx -x$ when x is small
3. Assumed x is small
4. Approximated $\frac{m(m-1)}{2n} \approx \frac{m^2}{2n}$

(b) If we halved the size of the hash table, how would the collision probability change? Recall $m \leq \sqrt{2n \cdot ln(1/p)}$.
Solving for p as a function of m and n:

$$p \leq e^{-\frac{m^2}{2n}}$$

If n is halved, the exponent doubles. Then, we could write:

$$\begin{aligned} p_{new} \leq e^{-\frac{2m^2}{2n}} &= (e^{-\frac{m^2}{2n}})^2 \\ &= p_{old}^2 \end{aligned}$$