CS 70 Midterm 2 Review

Shawn Mei, Edwin Liao, Sung Roa Yoon

Eta Kappa Nu, Mu Chapter
University of California, Berkeley

October 27 2012

Lagrange Interpolation

Given points (1, 0), (2, 1), (3, 0) over $GF(7)$, find the polynomial of degree 2 using Lagrange Interpolation.

Lagrange Interpolation

Given points (1, 0), (2, 1), (3, 0) over $GF(7)$, find the polynomial of degree 2 using Lagrange Interpolation.

$$\begin{aligned}
\Delta_1(x) &= \textit{Don't care!} \\
\Delta_2(x) &= \frac{(x-1)(x-3)}{(2-1)(2-3)} = -x^2 + 4x - 3 \\
\Delta_3(x) &= \textit{Don't care!} \\
p(x) &= 0 \cdot \delta_1 + 1 \cdot \delta_2 + 0 \cdot \delta_3 = -x^2 + 4x - 3 = 6x^2 + 4x + 4
\end{aligned}$$

Polynomial Counting

For a polynomial over $GF(p)$,

- How many unique lines (polynomials of at most degree $d = 1$) are there (given no points)?
- How many unique polynomials of (at most) degree d are there?
- Given $d - n$ fixed points, how many unique polynomials of (at most) degree d are there?

Polynomial Counting

For a polynomial over $GF(p)$,

- How many unique lines (polynomials of at most degree $d = 1$) are there (given no points)?

  p^2. Every line in a Galois field can be represented by 2 points, which can both take on p values. Remember that in a Galois field, a function $f(x)$ must have a value between 0 and $p - 1$, and thus any unique line can be defined by any two points that take on values $[0, p - 1]$

- How many unique polynomials of (at most) degree d are there?

- Given $d - n$ fixed points, how many unique polynomials of (at most) degree d are there?

Polynomial Counting

For a polynomial over $GF(p)$,

- How many unique lines (polynomials of at most degree $d = 1$) are there (given no points)?

  p^2. Every line in a Galois field can be represented by 2 points, which can both take on p values. Remember that in a Galois field, a function $f(x)$ must have a value between 0 and $p - 1$, and thus any unique line can be defined by any two points that take on values $[0, p - 1]$

- How many unique polynomials of (at most) degree d are there?

  p^{d+1}. This is because $d + 1$ points are needed to define a unique polynomial of degree d, and each of these points can take on p values.

- Given $d - n$ fixed points, how many unique polynomials of (at most) degree d are there?

Polynomial Counting

For a polynomial over $GF(p)$,

- How many unique lines (polynomials of at most degree $d = 1$) are there (given no points)?

  p^2. Every line in a Galois field can be represented by 2 points, which can both take on p values. Remember that in a Galois field, a function $f(x)$ must have a value between 0 and $p - 1$, and thus any unique line can be defined by any two points that take on values $[0, p - 1]$

- How many unique polynomials of (at most) degree d are there?

  p^{d+1}. This is because $d + 1$ points are needed to define a unique polynomial of degree d, and each of these points can take on p values.

- Given $d - n$ fixed points, how many unique polynomials of (at most) degree d are there?

  p^{n+1}. Building off the previous question, $d + 1$ points are still required, but $d - n$ points have been defined, leaving $n + 1$ undefined points that could each take on p values.

Heirarchical Secret Sharing

- Construct a secret-sharing scheme such that 15 people, 3 groups of 5, have a secret that can be found by a majority of group consent (≥ 2 groups). Group consent is by majority of members.

Heirarchical Secret Sharing

- Construct a secret-sharing scheme such that 15 people, 3 groups of 5, have a secret that can be found by a majority of group consent (≥ 2 groups). Group consent is by majority of members.

  Construct 2 secret-sharing schemes, one for the 3 groups and one for the members within the groups. The secret s_n for group n corresponds to a degree 2 polynomial $P_n(x) = ax^2 + bx + c$ with each group member m getting a share $(m, P_n(m))$, and secret $s_n = P_n(0)$. Then on the group level, the overall secret r for the entire 15 people will correspond to a degree 1 polynomial $Q(x) = dx + e$, where $Q(0) = r$ and the share for group n is (n, s_n).

Heirarchical Secret Sharing

- Construct a secret-sharing scheme such that 15 people, 3 groups of 5, have a secret that can be found by a majority of group consent (≥ 2 groups). Group consent is by majority of members.

  Construct 2 secret-sharing schemes, one for the 3 groups and one for the members within the groups. The secret s_n for group n corresponds to a degree 2 polynomial $P_n(x) = ax^2 + bx + c$ with each group member m getting a share $(m, P_n(m))$, and secret $s_n = P_n(0)$. Then on the group level, the overall secret r for the entire 15 people will correspond to a degree 1 polynomial $Q(x) = dx + e$, where $Q(0) = r$ and the share for group n is (n, s_n).
- Modify the solution so that a group leader (each group gets one leader) can give consent for the whole group, but three of the four remaining members can still override the leader if the leader declines.

Heirarchical Secret Sharing

- Construct a secret-sharing scheme such that 15 people, 3 groups of 5, have a secret that can be found by a majority of group consent (≥ 2 groups). Group consent is by majority of members.

  Construct 2 secret-sharing schemes, one for the 3 groups and one for the members within the groups. The secret s_n for group n corresponds to a degree 2 polynomial $P_n(x) = ax^2 + bx + c$ with each group member m getting a share $(m, P_n(m))$, and secret $s_n = P_n(0)$. Then on the group level, the overall secret r for the entire 15 people will correspond to a degree 1 polynomial $Q(x) = dx + e$, where $Q(0) = r$ and the share for group n is (n, s_n).
- Modify the solution so that a group leader (each group gets one leader) can give consent for the whole group, but three of the four remaining members can still override the leader if the leader declines.

  Give out 3 shares to the group leaders. This means the group leaders can construct their group's polynomial by themselves. No change is needed to the original group's polynomial P_n because 3 members still need to get together, which indicates a degree 2 polynomial.

Error Correcting

The message you want to send is 'BAD'. (Packets can take on letters from A to F, so represent letters as numbers in the range [0, 6] with $GF(7)$. Assume that the message receiver knows that the message is of length 3.) Construct the message such that it is protected against:

- 2 erasure errors.
- 2 corruption errors

Error Correcting

The message you want to send is 'BAD'. (Packets can take on letters from A to F, so represent letters as numbers in the range [0, 6] with $GF(7)$. Assume that the message receiver knows that the message is of length 3.) Construct the message such that it is protected against:

- 2 erasure errors.

  We will construct the polynomial $P(X)$ where $P(0) = 1, P(1) = 0, P(2) = 3$. By polynomial interpolation, we get $P(x) = 2x^2 + 4x + 1$. To protect against 2 erasure errors, we simply have to send two more packets. The message sent is $P(0), P(1), P(2), P(3), P(4)$, or [1, 0, 3, 4, 0], or $B_0A_1D_2E_3$. (Notation here is not standard - the subscript simply indicates the value of x by which the character was generated in the polynomial. The characters would be sent as pairs with their indices).

- 2 corruption errors

Error Correcting

The message you want to send is 'BAD'. (Packets can take on letters from A to F, so represent letters as numbers in the range [0, 6] with $GF(7)$. Assume that the message receiver knows that the message is of length 3.) Construct the message such that it is protected against:

- 2 erasure errors.

  We will construct the polynomial $P(X)$ where $P(0) = 1, P(1) = 0, P(2) = 3$. By polynomial interpolation, we get $P(x) = 2x^2 + 4x + 1$. To protect against 2 erasure errors, we simply have to send two more packets. The message sent is $P(0), P(1), P(2), P(3), P(4)$, or [1, 0, 3, 4, 0], or $B_0A_1D_2E_3$. (Notation here is not standard - the subscript simply indicates the value of x by which the character was generated in the polynomial. The characters would be sent as pairs with their indices).

- 2 corruption errors

  Send 4 more packets to compensate for corruption errors. $P(0), P(1), P(2), P(3), P(4), P(5), P(6)$ is [1, 0, 3, 4, 0, 1, 6] or $B_0A_1D_2E_3B_5F_6$

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?

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?

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?

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

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?

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?

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

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

Do all hypercubes have an Eulerian cycle?

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

Do all hypercubes have an Eulerian cycle?

No. A hypercube of dimension d has an Eulerian cycle iff d is even.

Winning the Lottery

The Mega Millions lottery drawing on March 30, 2012 had a jackpot of $656 million - the largest in American lottery history. Here are the basics of the lottery's rules: to buy a $1 lottery ticket, a player must choose 5 distinct numbers from 1 through 56 and 1 Mega number from 1 and 46. On the day of the lottery drawing, 5 distinct numbers from 1 through 56 and 1 Mega number from 1 and 46 are chosen as the winning numbers.

Winning the Lottery

The Mega Millions lottery drawing on March 30, 2012 had a jackpot of $656 million - the largest in American lottery history. Here are the basics of the lottery's rules: to buy a $1 lottery ticket, a player must choose 5 distinct numbers from 1 through 56 and 1 Mega number from 1 and 46. On the day of the lottery drawing, 5 distinct numbers from 1 through 56 and 1 Mega number from 1 and 46 are chosen as the winning numbers.

(a) What is the probability that someone buys a single lottery ticket and wins the jackpot by matching all 6 of the chosen numbers (the 5 normal numbers and the single Mega number)?

(b) On March 30, 2012, I found out that one of my lottery tickets was worth $3: exacty one of the normal numbers matched and the Mega number matched. What is the probability that someone who buys 1 lottery ticket wins $3? Don't bother simplifying your answer.

Winning the Lottery

The Mega Millions lottery drawing on March 30, 2012 had a jackpot of $656 million - the largest in American lottery history. Here are the basics of the lottery's rules: to buy a $1 lottery ticket, a player must choose 5 distinct numbers from 1 through 56 and 1 Mega number from 1 and 46. On the day of the lottery drawing, 5 distinct numbers from 1 through 56 and 1 Mega number from 1 and 46 are chosen as the winning numbers.

(a) What is the probability that someone buys a single lottery ticket and wins the jackpot by matching all 6 of the chosen numbers (the 5 normal numbers and the single Mega number)?

$$\frac{1}{\binom{56}{5} \times 46} = \frac{1}{175711536} = 5.69 \times 10^{-9}$$

(b) On March 30, 2012, I found out that one of my lottery tickets was worth $3: exacty one of the normal numbers matched and the Mega number matched. What is the probability that someone who buys 1 lottery ticket wins $3? Don't bother simplifying your answer.

Winning the Lottery

The Mega Millions lottery drawing on March 30, 2012 had a jackpot of $656 million - the largest in American lottery history. Here are the basics of the lottery's rules: to buy a $1 lottery ticket, a player must choose 5 distinct numbers from 1 through 56 and 1 Mega number from 1 and 46. On the day of the lottery drawing, 5 distinct numbers from 1 through 56 and 1 Mega number from 1 and 46 are chosen as the winning numbers.

(a) What is the probability that someone buys a single lottery ticket and wins the jackpot by matching all 6 of the chosen numbers (the 5 normal numbers and the single Mega number)?

$$\frac{1}{\binom{56}{5} \times 46} = \frac{1}{175711536} = 5.69 \times 10^{-9}$$

(b) On March 30, 2012, I found out that one of my lottery tickets was worth $3: exacty one of the normal numbers matched and the Mega number matched. What is the probability that someone who buys 1 lottery ticket wins $3? Don't bother simplifying your answer.

$$\frac{\binom{51}{4}\binom{5}{1}\binom{1}{1}}{\binom{56}{5}46}$$

Winning the Lottery (cont.)

(c) Let p be the probability that a lottery ticket is worth some positive amount of prize money. On March 30, 2012, I checked all 140 of my lottery tickets to see if any of them were worth anything. Luckily for me, two of them were. What is the probability that, if someone buys 140 lottery tickets, exactly two of them can be traded in for prize money?

Winning the Lottery (cont.)

(c) Let p be the probability that a lottery ticket is worth some positive amount of prize money. On March 30, 2012, I checked all 140 of my lottery tickets to see if any of them were worth anything. Luckily for me, two of them were. What is the probability that, if someone buys 140 lottery tickets, exactly two of them can be traded in for prize money?
$(1-p)^{138} \times p^2 \times \binom{140}{2}$

Go Vote!

With the U.S. presidential election coming up, it's important for us to remember how the election work. For the 2012 election, presidential candidates Barack Obama and Mitt Romney will fight for 538 electoral votes - whoever wins at least 270 of them wins the election. Assume that any state can split its votes among multiple candidates.

Go Vote!

With the U.S. presidential election coming up, it's important for us to remember how the election work. For the 2012 election, presidential candidates Barack Obama and Mitt Romney will fight for 538 electoral votes - whoever wins at least 270 of them wins the election. Assume that any state can split its votes among multiple candidates.

(a) How many ways can the two candidates split the 538 electoral votes? Ignore where (i.e. which state) each electoral vote came - we only care about the final outcome. For example, three possible electoral vote splits between Obama and Romney are:

(Obama, Romney) win (288, 250) votes respectively
(Obama, Romney) win (269, 269) votes respectively
(Obama, Romney) win (250, 288) votes respectively

Go Vote!

With the U.S. presidential election coming up, it's important for us to remember how the election work. For the 2012 election, presidential candidates Barack Obama and Mitt Romney will fight for 538 electoral votes - whoever wins at least 270 of them wins the election. Assume that any state can split its votes among multiple candidates.

(a) How many ways can the two candidates split the 538 electoral votes? Ignore where (i.e. which state) each electoral vote came - we only care about the final outcome. For example, three possible electoral vote splits between Obama and Romney are:

(Obama, Romney) win (288, 250) votes respectively
(Obama, Romney) win (269, 269) votes respectively
(Obama, Romney) win (250, 288) votes respectively

539: Each candidate can receive anywhere from 0 to 538 electoral votes.

Go Vote! (cont.)

(b) As of October 25, 2012, the Youtube video "Gangnam Style" by South Korean musician PSY has over half a billion views. By November 6, PSY has become so popular that he is now a viable candidate for the United States presidency. How many ways can 538 electoral votes be split among these three candidates?

(c) How many ways can 538 electoral votes be split among these three candidates if each candidate must receive at least one vote?

Go Vote! (cont.)

(b) As of October 25, 2012, the Youtube video "Gangnam Style" by South Korean musician PSY has over half a billion views. By November 6, PSY has become so popular that he is now a viable candidate for the United States presidency. How many ways can 538 electoral votes be split among these three candidates?
$\binom{538+2}{2} = \binom{540}{2}$

(c) How many ways can 538 electoral votes be split among these three candidates if each candidate must receive at least one vote?

Go Vote! (cont.)

(b) As of October 25, 2012, the Youtube video "Gangnam Style" by South Korean musician PSY has over half a billion views. By November 6, PSY has become so popular that he is now a viable candidate for the United States presidency. How many ways can 538 electoral votes be split among these three candidates?
$\binom{538+2}{2} = \binom{540}{2}$

(c) How many ways can 538 electoral votes be split among these three candidates if each candidate must receive at least one vote?
$\binom{537}{2}$

Go Vote! (cont.)

(d) If there are n presidential candidates and k votes, and presidential candidates **can** receive zero votes, how many ways can the electoral votes be split?

(e) If there are n presidential candidates and k votes, and presidential candidates **cannot** receive zero votes, how many ways can the electoral votes be split?

Go Vote! (cont.)

(d) If there are n presidential candidates and k votes, and presidential candidates **can** receive zero votes, how many ways can the electoral votes be split?
$\binom{n+k-1}{n-1}$

(e) If there are n presidential candidates and k votes, and presidential candidates **cannot** receive zero votes, how many ways can the electoral votes be split?

Go Vote! (cont.)

(d) If there are n presidential candidates and k votes, and presidential candidates **can** receive zero votes, how many ways can the electoral votes be split?
$\binom{n+k-1}{n-1}$

(e) If there are n presidential candidates and k votes, and presidential candidates **cannot** receive zero votes, how many ways can the electoral votes be split?
$\binom{k-1}{n-1}$

En Taro Tassadar

A normal Starcraft II player has a 20% chance of microing High Templars properly while a professional Starcraft II player has 99% chance of microing High Templars properly. If the player base is composed of 95% normal players and 5% professional players, and you observe that a random player can micro High Templars properly, what is the probability that the person is a professional player?

En Taro Tassadar

A normal Starcraft II player has a 20% chance of microing High Templars properly while a professional Starcraft II player has 99% chance of microing High Templars properly. If the player base is composed of 95% normal players and 5% professional players, and you observe that a random player can micro High Templars properly, what is the probability that the person is a professional player?

The probability that the person is a professional player given that he can micro High Templars properly would be:

En Taro Tassadar

A normal Starcraft II player has a 20% chance of microing High Templars properly while a professional Starcraft II player has 99% chance of microing High Templars properly. If the player base is composed of 95% normal players and 5% professional players, and you observe that a random player can micro High Templars properly, what is the probability that the person is a professional player?

The probability that the person is a professional player given that he can micro High Templars properly would be:

$$Pr[Prof|HT] = \frac{Pr[Prof \cap HT]}{Pr[HT]}$$

$$Pr[Prof|HT] = \frac{Pr[Prof \cap HT]}{Pr[Prof \cap HT] + Pr[Normal \cap HT]}$$

$$Pr[Prof|HT] = \frac{0.05 * 0.99}{0.05 * 0.99 + 0.95 * 0.20}$$

$$Pr[Prof|HT] = \frac{0.0495}{0.2395}$$

$$Pr[Prof|HT] \approx 0.21$$

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.

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.

$$Pr[A] = 1/3$$

$$Pr[B|A] = .2$$

$$Pr[B|\neg A] = .2$$

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

$$Pr[A|B] = \frac{0.2 * 0.33}{0.2 * 0.33 + 0.2 * 0.67}$$

$$Pr[A|B] = 0.33$$

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.

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

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.

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

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.

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

$$Pr[D] = 0.26$$

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

$$Pr[E] = 0.13$$

Theory

A and B are independent events $\iff Pr[A \cap B] = Pr[A] * Pr[B]$

$A_1, A_2, A_3, \cdots$ are mutually independent $\iff Pr[\cap_{i \in I} A_i] = \prod_{i \in I} Pr[A_i]$

Theory

A and B are independent events $\iff Pr[A \cap B] = Pr[A] * Pr[B]$

$A_1, A_2, A_3, \cdots$ are mutually independent $\iff Pr[\cap_{i \in I} A_i] = \prod_{i \in I} Pr[A_i]$

Example: You have 100 dice, you throw them all.

Theory

A and B are independent events $\iff Pr[A \cap B] = Pr[A] * Pr[B]$
$A_1, A_2, A_3, \cdots$ are mutually independent $\iff Pr[\cap_{i \in I} A_i] = \prod_{i \in I} Pr[A_i]$
Example: You have 100 dice, you throw them all.

Pairwise Independence: $Pr[A_i | \cap_{j \in I; j \neq i} A_j] = Pr[A_i]$

Theory

A and B are independent events $\iff Pr[A \cap B] = Pr[A] * Pr[B]$
$A_1, A_2, A_3, \cdots$ are mutually independent $\iff Pr[\cap_{i \in I} A_i] = \prod_{i \in I} Pr[A_i]$
Example: You have 100 dice, you throw them all.

Pairwise Independence: $Pr[A_i | \cap_{j \in I; j \neq i} A_j] = Pr[A_i]$
Example: You have two coins, you toss them both. X is probability of getting head on the first coin, Y is the prob. of getting head on second coin, and Z is the probability of the two being different. X, Y, Z are pairwise independent, but not mutually independent.

Theory

A and B are independent events $\iff Pr[A \cap B] = Pr[A] * Pr[B]$
$A_1, A_2, A_3, \cdots$ are mutually independent $\iff Pr[\cap_{i \in I} A_i] = \prod_{i \in I} Pr[A_i]$
Example: You have 100 dice, you throw them all.

Pairwise Independence: $Pr[A_i | \cap_{j \in I; j \neq i} A_j] = Pr[A_i]$
Example: You have two coins, you toss them both. X is probability of getting head on the first coin, Y is the prob. of getting head on second coin, and Z is the probability of the two being different. X, Y, Z are pairwise independent, but not mutually independent.

Product Rule: $Pr[\cap_{i=1}^{n} A_i] = Pr[A_1] * Pr[A_2|A_1] * ... * Pr[A_n | \cap_{i \in \{1,...,n-1\}} A_i$

Theory

A and B are independent events $\iff Pr[A \cap B] = Pr[A] * Pr[B]$
$A_1, A_2, A_3, \cdots$ are mutually independent $\iff Pr[\cap_{i \in I} A_i] = \prod_{i \in I} Pr[A_i]$
Example: You have 100 dice, you throw them all.

Pairwise Independence: $Pr[A_i | \cap_{j \in I; j \neq i} A_j] = Pr[A_i]$
Example: You have two coins, you toss them both. X is probability of getting head on the first coin, Y is the prob. of getting head on second coin, and Z is the probability of the two being different. X, Y, Z are pairwise independent, but not mutually independent.

Product Rule: $Pr[\cap_{i=1}^{n} A_i] = Pr[A_1] * Pr[A_2|A_1] * ... * Pr[A_n | \cap_{i \in \{1,\ldots,n-1\}} A_i$

Principle of Inclusion/Exclusion:
$Pr[\cup_{i=1}^{n} A_i] = \sum Pr[A_i] - \sum Pr[A_i \cap A_j] + Pr[A_i \cap A_j \cap A_k] - ...$

Theory

A and B are independent events $\iff Pr[A \cap B] = Pr[A] * Pr[B]$
$A_1, A_2, A_3, \cdots$ are mutually independent $\iff Pr[\cap_{i \in I} A_i] = \prod_{i \in I} Pr[A_i]$
Example: You have 100 dice, you throw them all.

Pairwise Independence: $Pr[A_i | \cap_{j \in I; j \neq i} A_j] = Pr[A_i]$
Example: You have two coins, you toss them both. X is probability of getting head on the first coin, Y is the prob. of getting head on second coin, and Z is the probability of the two being different. X, Y, Z are pairwise independent, but not mutually independent.

Product Rule: $Pr[\cap_{i=1}^{n} A_i] = Pr[A_1] * Pr[A_2|A_1] * ... * Pr[A_n | \cap_{i \in \{1,\ldots,n-1\}} A_i$

Principle of Inclusion/Exclusion:
$Pr[\cup_{i=1}^{n} A_i] = \sum Pr[A_i] - \sum Pr[A_i \cap A_j] + Pr[A_i \cap A_j \cap A_k] - ...$

Disjoint Events: $Pr[\cup_{i=1}^{n} A_i] = \sum_{i=1}^{n} Pr[A_i]$

Theory

A and B are independent events $\iff Pr[A \cap B] = Pr[A] * Pr[B]$
$A_1, A_2, A_3, \cdots$ are mutually independent $\iff Pr[\cap_{i \in I} A_i] = \prod_{i \in I} Pr[A_i]$
Example: You have 100 dice, you throw them all.

Pairwise Independence: $Pr[A_i | \cap_{j \in I; j \neq i} A_j] = Pr[A_i]$
Example: You have two coins, you toss them both. X is probability of getting head on the first coin, Y is the prob. of getting head on second coin, and Z is the probability of the two being different. X, Y, Z are pairwise independent, but not mutually independent.

Product Rule: $Pr[\cap_{i=1}^{n} A_i] = Pr[A_1] * Pr[A_2|A_1] * ... * Pr[A_n | \cap_{i \in \{1,...,n-1\}} A_i$

Principle of Inclusion/Exclusion:
$Pr[\cup_{i=1}^{n} A_i] = \sum Pr[A_i] - \sum Pr[A_i \cap A_j] + Pr[A_i \cap A_j \cap A_k] - ...$

Disjoint Events: $Pr[\cup_{i=1}^{n} A_i] = \sum_{i=1}^{n} Pr[A_i]$

Union: $Pr[\cup_{i=1}^{n} A_i] \leq \sum_{i=1}^{n} Pr[A_i]$

Independence Problems

You have three bits, and the three bits each have $p_i = 1/2$ probability of being set. If X is the probability of getting a 1 on the first bit, Y is the probability of getting a 1 on the second bit, and Z is the probability of XORing all three to have a value of 1, is there any independence relationship between the three? If so, mutual or pairwise?

Independence Problems

You have three bits, and the three bits each have $p_i = 1/2$ probability of being set. If X is the probability of getting a 1 on the first bit, Y is the probability of getting a 1 on the second bit, and Z is the probability of XORing all three to have a value of 1, is there any independence relationship between the three? If so, mutual or pairwise?

X: 1/2

Y: 1/2

Z: 1/2 regardless of whether you know X or Y.

Independence Problems

You have three bits, and the three bits each have $p_i = 1/2$ probability of being set. If X is the probability of getting a 1 on the first bit, Y is the probability of getting a 1 on the second bit, and Z is the probability of XORing all three to have a value of 1, is there any independence relationship between the three? If so, mutual or pairwise?
X: 1/2
Y: 1/2
Z: 1/2 regardless of whether you know X or Y.

You have three bits, and the three bits each have $p_i \neq 1/2$ probability of being set. If X is the probability of getting a 1 on the first bit, Y is the probability of getting a 1 on the second bit, and Z is the probability of XORing all three to have a value of 1, is there mutual independence relationship between the three?

Independence Problems

You have three bits, and the three bits each have $p_i = 1/2$ probability of being set. If X is the probability of getting a 1 on the first bit, Y is the probability of getting a 1 on the second bit, and Z is the probability of XORing all three to have a value of 1, is there any independence relationship between the three? If so, mutual or pairwise?
X: 1/2
Y: 1/2
Z: 1/2 regardless of whether you know X or Y.

You have three bits, and the three bits each have $p_i \neq 1/2$ probability of being set. If X is the probability of getting a 1 on the first bit, Y is the probability of getting a 1 on the second bit, and Z is the probability of XORing all three to have a value of 1, is there mutual independence relationship between the three?
No.

Product Rule and Inclusion/Exclusion

If you toss a coin 5 times, what is the probability that you will get at least one head? Try solving this with product rule and again with the principle of inclusion/exclusion.

Product Rule and Inclusion/Exclusion

If you toss a coin 5 times, what is the probability that you will get at least one head? Try solving this with product rule and again with the principle of inclusion/exclusion.

Product: $Pr[H] = 1/2 + 1/2^2 + 1/2^3 + 1/2^4 + 1/2^5 = 0.96875$

Product Rule and Inclusion/Exclusion

If you toss a coin 5 times, what is the probability that you will get at least one head? Try solving this with product rule and again with the principle of inclusion/exclusion.

Product: $Pr[H] = 1/2 + 1/2^2 + 1/2^3 + 1/2^4 + 1/2^5 = 0.96875$

Inclusion/Exclusion:
$Pr[H] = 1/2 * 5 - 1/2^2 * 10 + 1/2^3 * 10 - 1/2^4 * 5 + 1/2^5 = 0.96875$

That's it!

Good luck on your midterm and thanks for coming!
Please fill out a feedback form before you leave!