Lecture 8 Notes

• Goals for Today
  – Counting
    • Partitions (Sterling #’s of second kind), functions
  – Probability
    • Random variables, expectation, variance
    • Birthday paradox
    • Random graphs
  – Other: Enigma machine, cardinalities, ...
    • “Basic Concepts and Notation” from UVA posted

• Generated questions on WeBWorK
  – Functions set is up today
  – “Worked-out solutions” can be viewed in WeBWorK!

• My OH’s tomorrow: questionable! (try for 10am please)

• Midterm next Thursday – closed book, no calculators
  – You are allowed 1 handwritten 8.5”x11” sheet of paper
  – Review session Tuesday 4/29 6:30-8:30pm, Ledden Hall
  – Practice MT questions + draft solution set are posted
### Ordered? With Repetition?
*(from RRR’s office hours)*

<table>
<thead>
<tr>
<th></th>
<th>No Repetition (without replacement)</th>
<th>With Repetition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Order Matters</td>
<td><strong>$P(n,k)$</strong> #k-lists from n-set</td>
<td><strong>$n^k$</strong> #k-lists from n-set</td>
</tr>
<tr>
<td></td>
<td>**$P(</td>
<td>B</td>
</tr>
</tbody>
</table>
| Order Doesn’t Matter | **$C(n,k)$** #k-sets from n-set; binomial coefficients | **$C(n + k – 1, k – 1)$**
| (select, choose)|                                    | $n$ indistinguishable objects in $k$
|                |                                     | marked boxes ($\equiv$ selecting one of $k$
|                |                                     | boxes, $n$ times with repetition); order form (n hotdogs, k flavors) |
**Counting Functions, Injections**

- How many functions are there from a 3-set to a 7-set? $7^3$

- How many functions are there from a 7-set to a 3-set? $3^7$

* If I asked: surjections?  

- How many injections are there from a 3-set to a 7-set? \( \binom{7}{3} = 7! / 4! = 7 \cdot 6 \cdot 5 \)

- How many injections are there from a 7-set to a 3-set? 0
Number of Ways to Partition a Set

Example 24 (Set partitions) A partition of a set \( B \) is a collection of nonempty subsets of \( B \) such that each element of \( B \) appears in exactly one subset. Each subset is called a block of the partition. The 15 partitions of \( \{1, 2, 3, 4\} \) by number of blocks are

<table>
<thead>
<tr>
<th>1 block:</th>
<th>{{1, 2, 3, 4}}</th>
</tr>
</thead>
<tbody>
<tr>
<td>2 blocks:</td>
<td>{{1, 2, 3}, {4}} {{1, 2, 4}, {3}} {{1, 2}, {3, 4}} {{1, 3, 4}, {2}} {{1, 3}, {2, 4}} {{1, 4}, {2, 3}} {{1}, {2, 3, 4}}</td>
</tr>
<tr>
<td>3 blocks:</td>
<td>{{1, 2}, {3}, {4}} {{1, 3}, {2}, {4}} {{1, 4}, {2}, {3}} {{1}, {2, 3}, {4}} {{1}, {2}, {3, 4}}</td>
</tr>
<tr>
<td>4 blocks:</td>
<td>{{1}, {2}, {3}, {4}}</td>
</tr>
</tbody>
</table>

“Stirling numbers of the second kind”
- \( S(n,k) \) = number of ways to partition \( \{1, \ldots, n\} \) into exactly \( k \) nonempty subsets
- \( S(4,1) = 1 \)
- \( S(4,2) = 7 \)
- \( S(4,3) = 6 \)
- \( S(4,4) = 1 \)
Number of Ways to Partition a Set

1 block: \{\{1, 2, 3, 4\}\}
2 blocks: \{\{1, 2, 3\}, \{4\}\}  \{\{1, 2, 4\}, \{3\}\}  \{\{1, 2\}, \{3, 4\}\}  \{\{1, 3, 4\}, \{2\}\}
             \{\{1, 3\}, \{2, 4\}\}  \{\{1, 4\}, \{2, 3\}\}  \{\{1\}, \{2, 3, 4\}\}
3 blocks: \{\{1, 2\}, \{3\}, \{4\}\}  \{\{1, 3\}, \{2\}, \{4\}\}  \{\{1, 4\}, \{2\}, \{3\}\}  \{\{1\}, \{2, 3\}, \{4\}\}
             \{\{1\}, \{2, 4\}, \{3\}\}  \{\{1\}, \{2\}, \{3, 4\}\}
4 blocks: \{\{1\}, \{2\}, \{3\}, \{4\}\}

- \(S(n,k)\) = number of ways to partition \{1, \ldots, n\} into exactly \(k\) nonempty subsets
- Observations:
  - \(S(n,1) = 1\) \(\forall n\)
  - \(S(n,n) = 1\) \(\forall n\)
  - \(S(n,2) = ?\)
    - \(2^{n-1} - 1\)
  - \(S(n,n-1) = ?\)
    - \(C(n,2)\)

\[
\sum_{k=1}^{n/2} C(n, k) = 2^n
\]

\[
\frac{2^n - 2}{2}
\]

\(\)
Number of Ways to Partition a Set

- $S(n,k)$ = number of ways to partition $\{1, \ldots, n\}$ into exactly $k$ nonempty subsets
- What is $S(5,2)$?
  - Add “5” to all $S(4,1)$ partitions into 1 blocks
  - Add “5” to all $S(4,2)$ partitions into 2 blocks

$S(4,1) = 1$

$S(4,2) = 7$

$S(4,3) = 6$

$S(4,4) = 1$

Idea: work from $S(4,1)$ and $S(4,2)$

- New number is a brand-new block by itself
- $\{1,2,3,4\}, \{5\}$

- Or $\{1,3,5\}, \{2,4\}$

$C(n,k) = C(n-1,k) + C(n-1,k-1)$

Number of Ways to Partition a Set

- S(n,k) = number of ways to partition \{1, \ldots, n\} into exactly k nonempty subsets
- What is S(5,3)?
  - Add “5” to all S(4,2) partitions into 2 blocks
    - 6 partitions * 3 ways = 18 ways
  - Add “5” to all S(4,3) partitions into 3 blocks
    - 7 partitions

S(5,3) = 7 + 18 = 25
Number of Ways to Partition a Set

- \( S(n,k) \) = number of ways to partition \{1, \ldots, n\} into exactly \( k \) nonempty subsets
- Recursion:

\[
S(n,k) = S(n-1, k-1) + k \cdot S(n-1, k)
\]
From Last Time

• How many functions from \{1, 2, 3, 4\} to \{a, b, c, d, e\} have exactly \textbf{two} elements in the image?

• Case 1: \(4 = 1 + 3\)

\[
C(4,1) \cdot C(5,1) \cdot C(3,3) \cdot C(4,1) = C(4,1) \cdot C(3,3) \cdot C(5,2) \cdot 2 = 80
\]
From Last Time

- Recall: How many functions from \{1, 2, 3, 4\} to \{a, b, c, d, e\} have exactly **two** elements in the image?

- Case 1:  \[4 = 2 + 2\]

\[
\binom{4}{2} \cdot \binom{5}{2} = 60
\]

\[
= \binom{4}{2} \cdot \binom{5}{1} \cdot \binom{2}{2} \cdot \binom{4}{1} / 2 = 60
\]

picking (1,2) \(\rightarrow\) a (implying (3,4) \(\rightarrow\) d) is same as picking (3,4) \(\rightarrow\) d (implying (1,2) \(\rightarrow\) a)
Counting Surjections

- Previous example: $S(4,2) = 7$
- Multiply by $5 \cdot 4$ (= choosing 2 elements of image in $B$)
- $7 \cdot 5 \cdot 4 = 140 = 80 + 60$

- So ... number of surjections from $|A|$ to $|B|$, given that $|A| \geq |B|$?
  
  $S(|A|, |B|) \cdot (|B|)!$

$S(|A|, |B|)$ is the number of surjections from $|A|$ to $|B|$, and $(|B|)!$ represents the number of ways to arrange $|B|$ elements.

Diagram:

- Set $A$ with elements 1, 2, 3, 4
- Set $B$ with elements a, b, c, d, e
- Surjections from $A$ to $B$: a, b, c, d, e
- $S(|A|, |B|)$ represents the number of surjections from $|A|$ to $|B|$.
- $(|B|)!$ represents the arrangements of elements in $B$. 

Note: $B!$ ways indicate the arrangements of elements in $B$. 

$\# \text{partitions of } A \text{ into } |B| \text{ blocks} = S(|A|, |B|)$
A Probability Question

• What is the probability that a random function from \( \{1, 2, 3, 4\} \) to \( \{a, b, c, d, e\} \) has exactly two elements in its range?

• \(|5|^4| = 625 \) total functions
• \(140 / 625 = 0.224\)
Sampling With, Without Replacement

• Given an urn with 5 marbles: 2 white and 3 red

• Draw one marble at random, record its color, then replace. Then draw a second one. What is the probability that the second one is red? \( \frac{3}{5} \)

\[ U = \{(m_1, m_2) \mid m_i \in \{R_1, R_2, R_3, W_4, W_5\}\} \]

• Draw one out, record color, then throw away. Then draw a second one. If the first one is white, what is the probability that the second one is red? \( \frac{3}{4} \)

\[ P(\{(W, R_i)\}) = \frac{3}{4} \]

• Draw one out, don’t look at color, throw it away and draw a second one. What is the probability that the second one is red?

\[ \frac{2}{5} \cdot \frac{3}{4} + \frac{3}{5} \cdot \frac{2}{4} = \frac{3}{5} \]

cf. “Law of Total Probability”
Sampling With, Without Replacement

• Betting on a six-horse horse race.

• Buy six tickets, each on a different horse
  \( Without \text{ replacement} \)
  \[ Pr = 1 \]

• Buy six tickets, each time randomly choosing a horse
  \( With \text{ replacement} \)
  \[ 1 - Pr(\text{no winning tickets}) = 1 - \left(\frac{5}{6}\right)^6 \]

• What is the probability that at least one of the tickets picks the winning horse?
iClicker Quiz, Week 4

Q1: Let A and B be events with \( P(A) = \frac{6}{15} \), \( P(B) = \frac{8}{15} \), and \( P((A \cup B)^c) = \frac{3}{15} \). What is \( P(A \cap B) \)?
   A: \( \frac{1}{15} \)  B: \( \frac{2}{15} \)  C: \( \frac{3}{15} \)  D: \( \frac{4}{15} \)  E: \( \frac{5}{15} \)

Q2: A permutation on \( \{1, 2, \ldots, 8\} \) is expressed in cycle form as \((1,3,4)(2,8,6)\). Which of the following correctly represents the inverse permutation?
   A: \((4,3,1)(2,8,6)\)  B: \((3,1,4)(6,8,2)\)  C: \((6,8,2,4,3,1)\)  D: \((5)(7)\)  E: \((1,3,4)(6,8,2)\)

Q3: The correct answer is A.

Q4: The correct answer is C.
   A: ---  B: ---  C: ---  D: ---  E: ---

Q5: (bonus) The correct answer is D.
   A: ---  B: ---  C: ---  D: ---  E: ---
Another Probability Question

• In a room with $n$ people, what is the probability that some two people have the same birthday?
• Assume that all possible birthdays are equally likely, and there are only 365 of them.
• Let $A$ be the event that some two people in the same room have the same birthday.
• $P(A) = 1 - P(A^c)$

$A = \text{some two people have the same birthday}$

$A^c = \text{no two people have the same birthday}$
Birthdays

• $P(A) = 1 - P(A^c)$

• Let $B_i$ be the probability that person $i$ has a different birthday than persons 1, 2, ..., $i-1$

• Note: $B_1 = 1$
Birthdays

- Let’s try to calculate $P(A^c)$, the probability that no two people among 1, ..., $n$ have the same birthday:

  - $P(A^c) = B_1 \cdot B_2 \cdot ... \cdot B_n$

- What is $B_2$?

  - $B_2 = \frac{364}{365}$ because one birthday has been “taken” so far

- $B_i = \frac{365-i+1}{365}$
“The Birthday Paradox”

Let’s try to calculate \( P(A^c) \), the probability that no two people among 1, ..., \( n \) have the same birthday:

\[
P(A^c) = B_1 \cdot B_2 \cdot ... \cdot B_n
\]

\[
P(A^c) = \left( \frac{365}{365} \right) \left( \frac{364}{365} \right) \left( \frac{363}{365} \right) ... \left( \frac{365-n+1}{365} \right)
\]

\[
= \frac{365!}{365^n(365-n)!}
\]

What is \( P(A^c) \) when \( n = 1 \)?

What is \( P(A^c) \) when \( n = 23 \)?

\[
\frac{365!}{365^{23}(342)!} \approx 0.4927
\]

Pr = 0.5073

that two students have same birthday

Pr = 1
Closing the Loop

• “No birthday gets hit twice …” reminds you of …

• … an injection!

• Probability that a random function from \{1, 2, 3, \ldots, n\} to \{1, 2, 3, 4, \ldots, 364, 365\} is an injection is …

\[
\frac{(365! / (365-n)!) / 365^n}{365^n}
\]
Random Variables

• Definition. Given a probability space \((U, P)\), we say that the function \(X: U \to \mathbb{R}\) is a random variable
  – \(X\) associates numerical values with elements of the sample space

• Example. Flip a fair coin four times. Some associated random variables:
  – \(X = \) number of heads that appear
  – \(Y = \) result of second flip
  – \(Z = \) number of switches from H to T or vice versa

• What are possible values of \(X\)?
• What are possible values of \(Y\)?
• What are possible values of \(Z\)?

Each value of a given random variable corresponds to an event (subset of \(U\)).
Mean or Expected Value

- Mean value = expected value of one sample from a random variable
  - i.e., “average”
- If the random variable X can take values $x_1, x_2, \ldots, x_n$ with respective probabilities $p_1, p_2, \ldots, p_n$, then the mean or expected value of X, written $E[X]$, is

$$E[X] = \sum_{k=1}^{n}(pkx_k)$$
Expected Value

• Suppose that the random variable X takes on values \(\{x_1=1, x_2=2, x_3=3, x_4=4, x_5=5\}\) with probabilities

\[
\begin{align*}
p_1 &= P(X = x_1) = .05 \\
p_2 &= P(X = x_2) = .05 \\
p_3 &= P(X = x_3) = .2 \\
p_4 &= P(X = x_4) = .3 \\
p_5 &= P(X = x_5) = .4
\end{align*}
\]

Then \(E[X] = \sum_{k=1}^{5} (p_k x_k) = \)

\[
= (1)(.05) + (2)(.05) + (3)(.2) + (4)(.3) + (5)(.4)
\]

\(= 3.95\)
Variance

• Definition: The variance of a random variable is

$$\sigma_x^2 = \text{Var}(X) = E(X^2) - (E(X))^2$$

• Expected value of $X^2$, minus (expected value of $X$), squared

• Variance how much $X$ is likely to vary through its distribution.
Variance Example

• Again: $X$ takes values \{x_1=1, x_2=2, x_3=3, x_4=4, x_5=5\} with probabilities:

  
  \begin{align*}
  p_1 &= P(X = x_1) = .05 \\
p_2 &= P(X = x_2) = .05 \\
p_3 &= P(X = x_3) = .2 \\
p_4 &= P(X = x_4) = .3 \\
p_5 &= P(X = x_5) = .4 \\
  \end{align*}

\[E[X^2] = \sum_{k=1}^{5} (pk \cdot k^2) = (1)(.05) + (4)(.05) + (9)(.2) + (16)(.3) + (25)(.4) = 16.85\]

\[E[X] = 3.95 \text{ from before}\]

\[\text{Var}(X) = E(X^2) - (E(X))^2 = 16.85 - (3.95)^2 = 1.2475\]
Graphs

Gene-gene interactions affecting phenotype in yeast
Graphs

Airline routes

Control/data flow graph
Graph Representation

- Graph $G = (V,E)$
  - Vertex set $V = V(G)$  $V = \{1, 2, 3, 4, 5\}$
  - Edge set $E = E(G)$ (connecting pairs of vertices)
    $E = \{(1,3), (1,4), (2,3), (2,4), (3,5), (4,5)\}$

- There is a HW 4 question is on random graphs
- Class $G(n,p)$ of random graphs:
  - $|V| = n$ vertices
  - Every edge $e = (v_i,v_j)$ exists independently, with $\text{Prob}(e) = p$
Graphs

Internet topology
(random growth models have been proposed)
From Dr. Rubalcaba: basics of Enigma

Permutations of the Enigma

- plugboard: lots of complexity! \[ \cdot C(26,2) \cdot C(24,2) \cdot \ldots \]
Two Enigma Rotors

3 rotors:
- Right: 1 move per keystroke
- Middle: " " 26 moves of Right rotor
- Left: " " " " Middle " ""
Two Enigma Rotors (right rotor exploded view)

Each rotor: permutation on 26 letters
An Enigma Rotor (exploded view)

You can see the 26 wires that make up the function map from the set of letters \(\{A, B, \ldots, Z\}\) to \(\{A, B, \ldots, Z\}\). This function is a permutation (all Enigma rotors were permutations on 26 letters).
The Nine Permutations of the Enigma

Enter the stecker (plugboard) on the right, follow a wire through the stecker, right rotor, middle rotor, left rotor, Umkehrwalze (reflector plate), then backwards through the left, middle, right rotors and finally backwards through the plugboard.
Wiring of the Enigma (simple 4 letter, 3 rotor model)

“press A, light goes on at D”

A is pressed and D is illuminated (Note the plugboard wire swapping the roles of S and D)
Reading – Keywords!

• Random variables
• Distribution function of r.v.
• Expectation
• Variance
• Linearity of expectation
• Binomial distribution, Hypergeometric distribution
• Poisson distribution
• Normal distribution
• Joint distribution
• Marginal distribution
• Independence
Fun (from Lecture 6)

• If two sets can be put into 1-1 correspondence, their cardinalities are equal.

• “Cardinality” of infinite sets: very interesting!

*See the posted handout by Prof. Gabriel Robins, UVA

“Elvis’s Hotel”: although it’s always crowded, you still can find some room ...

Elvis’s Hotel has Rooms 1, 2, 3, … Every room is occupied by a guest.

- Room 1: occupied - Room $10^{38}$: occupied. Etc.

- One person arrives. Can he be accommodated?

  $\text{Is } |\mathbb{N} \cup \{\text{Bob}\}| >, =, < |\mathbb{N}|$?

- Five people arrive. Can they be accommodated?

- $|\mathbb{N}|$ people arrive. Can they be accommodated?

  $\text{Is } |\mathbb{Z}| >, =, < |\mathbb{N}|$?
Fun (from Lecture 6)
• If two sets can be put into 1-1 correspondence, their cardinalities are equal.
• Which set has larger cardinality:
  – R (reals) or (0,1) ? **SAME**
  – N (counting numbers) or N × N = Q⁺ (positive rationals) ?
  – N (counting numbers) or R⁺ (positive reals) ?
Problems 8

• P8.1 Prove that no matter how you place 33 rooks on an 8 x 8 chessboard, there will always be five of them that are mutually non-attacking.

• P8.2 Are you able to choose a set of 1983 (distinct) non-negative integers, all less than 100000, such that no three are in arithmetic progression? (Hint 1: What happens if you greedily construct such a set, starting with 0?  Hint 2: What does your set look like in ternary (base 3) notation?)

• P8.3 Start with two points on a line labeled 0, 1 in that order. In one move you may add or delete two neighboring points (0,0) or (1,1). Your goal is to reach a single pair of points labeled (1,0) in that order. Can you achieve this goal?
EXTRA
A man is dealt 4 spade cards from an ordinary deck of 52 cards. He is then given 2 more cards. Let \( x \) be the probability that both of these cards are of the same suit. Which is true?

- (a) \( 0.2 < x \leq 0.3 \)
- (b) \( 0 < x \leq 0.1 \)
- (c) \( 0.1 < x \leq 0.2 \)
- (d) \( 0.3 < x \leq 0.4 \)
- (e) \( 0.4 < x \leq 0.5 \)

\[
\binom{9}{2} + \binom{13}{2} + \binom{13}{2} + \binom{13}{2} \quad \frac{\binom{4}{8}}{2} \]
Probability Warmups

- You roll two fair dice. What is the probability that the greatest common divisor of the two numbers rolled is 1?

(a) $\frac{12}{36}$ (b) $\frac{15}{36}$ (c) $\frac{17}{36}$ (d) $\frac{19}{36}$ (e) $\frac{23}{36}$

$\begin{array}{ccc}
2-4 & 2-2 \\
2-6 & 3-3 \\
4-6 & 4-4 \\
3-6 & 5-5 \\
\end{array}$

$\times 2$

$36 - 13$ combinations

$= \frac{23}{36}$
Probability Warmups

• You are given a square with side $s$, and completely contained inside the square, a circle of radius $r < s$. A point is selected uniformly at random from the square. What is the probability that the selected point lies inside the circle?

\[
\frac{\pi r^2}{s^2}
\]
Probability Warmups

• You play a coin-tossing game in which you continue to flip a fair coin until it first turns up heads. Consider the potential third flip in this game.

• Given that the game reaches a third flip, what is a probability that the coin turns up heads on the third flip? \( \frac{1}{2} \)

• What is the probability that there is a third flip in the game, and that flip turns up heads? \( \frac{1}{8} \)