CMPT 210: Probability and Computation

Lecture 1

Sharan Vaswani

May 10, 2022

Course Information

- **Instructor**: Sharan Vaswani (TASC-1 9203) Email: `sharan_vaswani@sfu.ca`
- **Office Hours**: Tuesday 11 am - 12 pm (TASC-1 9203), Thursday 9 am - 10 am (ASB9808)
- **Teaching Assistants**: Yasaman Etesam, Aditya Bhadreshkumar Panchal
- **Course Webpage**: `https://vaswanis.github.io/210-S22`
- **Piazza**: `https://piazza.com/sfu.ca/summer2022/cmpt210/home`
- **Prerequisites**: MACM 101, MATH 152 and MATH 232/MATH 240

Course Information

Objective: Introduce the foundational concepts in probability required by computing.

Syllabus:

- Combinatorics, Set Theory, Inclusion-Exclusion.
- Probability theory, Random variables, Joint distributions.
- Expectation, Variance, Standard Deviation, Discrete distributions: Binomial and Geometric.
- Conditional probability, Bayes' Theorem, Tail inequalities (Markov, Chebyshev, Chernoff).
- Applications: Freivalds' algorithm, Quicksort, Max-cut, Load Balancing, A/B testing
- Normal Distribution, Central Limit Theorem (introduction)

Resources:

- Introduction to Probability and Statistics for Engineers and Scientists (Ross).
- Mathematics for Computer Science (Meyer, Lehman, Leighton): `https://people.csail.mit.edu/meyer/mcs.pdf`
- CMU Lecture Notes for Probability and Computing (O'Donnell): `http://www.cs.cmu.edu/~odonnell/papers/probability-and-computing-lecture-notes.pdf`

Course Information

- **Grading**:
  - 4 Assignments ($4 \times 12.5\% = 50\%$)
  - 1 Mid-Terms ($1 \times 15\% = 15\%$) (24 June)
  - 1 Final Exam ($1 \times 35\% = 35\%$) (TBD)

  - Each assignment is due in 1 week (typically Friday).
  - For some flexibility, each student is allowed 1 late-submission and can submit in the next class (typically the Tuesday after).
  - If you miss the mid-term (needs to be a well-justified reason), will reassign weight to the final.
  - If you miss the final, there will be a make-up exam.

Questions?

Sets

Informal def: Unordered collection of objects (referred to as *elements*)

Examples: $\{a, b, c\}$, $\{\{a, b\}, \{c, a\}\}$, $\{1.2, 2.5\}$, {yellow, red, green}, $\{x|x$ is capital of a North American country$\}$, $\{x|x$ is an integer in $[5, 10]\}$.

There is no notion of an element appearing twice. E.g. $\{a, a, b\} = \{a, b\}$.

The order of the elements does not matter. E.g. $A = \{a, b\} = \{b, a\}$.

C $= \{x|x$ is a color of the rainbow $\}$

Elements of C: red, orange, yellow, green, blue, indigo, violet.

Membership: red $\in C$, brown $\notin C$.

Cardinality: Number of elements in the set. $|C| = 7$

Q: A $= \{x|5 < x < 17$ and x is a power of 2 $\}$. Enumerate A. What is $|A|$?

Ans: $A = \{8, 16\}$, $|A| = 2$

Common Sets

- $\emptyset$ Empty Set
- $\mathbb{N}$ Set of nonnegative integers $\{0, 1, 2 \ldots\}$
- $\mathbb{Z}$ Set of integers $\{-2, -1, 0, 1, 2 \ldots\}$
- $\mathbb{Q}$ Set of rational numbers that can be expressed as p/q where $p, q \in \mathbb{Z}$ and $q \neq 0$. $\{-10.1, -1.2, 0, 5.5, 15 \ldots\}$
- $\mathbb{R}$ Set of real numbers $\{e, \pi, \sqrt{2}, 2, 5.4\}$
- $\mathbb{C}$ Set of complex numbers $\{2 + 5i, -i, 1, 23.3, \sqrt{2}\}$

Comparing sets: A is a subset of B ($A \subseteq B$) iff every element of A is an element of B. E.g. $A = \{a, b\}$ and $B = \{a, b, c\}$, then $A \subseteq B$. Every set is a subset of itself i.e. $A \subseteq A$.

A is a *proper* subset of B ($A \subset B$) iff A is a subset of B, and A is not equal to B,

Q: Is $\{1, 4, 2\} \subset \{2, 4, 1\}$. Is $\{1, 4, 2\} \subseteq \{2, 4, 1\}$ Ans: No, Yes
Q: Is $\mathbb{N} \subset \mathbb{Z}$? Is $\mathbb{C} \subset \mathbb{R}$? Ans: Yes, No
Q: What is $|\emptyset|$? Ans: 0

Set Operations

Union: The union of sets A and B consists of elements appearing in A OR B. If $A = \{1, 2, 3\}$ and $B = \{3, 4, 5\}$, then $A \cup B = \{1, 2, 3, 4, 5\}$.

Intersection: The intersection of sets A and B consists of elements that appear in both A AND B. If $A = \{1, 2, 3\}$ and $B = \{3, 4, 5\}$, then $A \cap B = \{3\}$.

Set difference: The set difference of A and B consists of all elements that are in A, but not in B. $A = \{1, 2, 3\}$ and $B = \{3, 4, 5\}$, then $A \backslash B = A - B = \{1, 2\}$. $B \backslash A = B - A = \{4, 5\}$.

Complement: Given a domain (or universe) D such that $A \subset D$, the complement of A consists of all elements that are not in A. $D = \mathbb{N}$, $A = \{1, 2, 3\}$. $A \subset D$ and $\bar{A} = \{0, 4, 5, 6, \ldots\}$.

$A \cup \bar{A} = D$, $A \cap \bar{A} = \emptyset$, $A \backslash \bar{A} = A$.

Q: $D = \mathbb{N}$, $A = \{1, 2, 3\}$ and $B = \{3, 4, 5\}$. Compute $\overline{A \cap B}$, $(B \backslash A) \cup (A \backslash B)$.

Ans: $\overline{A \cap B} = \{0, 1, 2, 4, 5, \ldots\}$, $(B \backslash A) \cup (A \backslash B) = \{1, 2, 4, 5\}$

Set operations and relations

Disjoint sets: Two sets are *disjoint* iff $A \cap B = \emptyset$.

Symmetric Difference: $A \Delta B$ is the set that contains those elements that are either in A or in B, but not in both.

Q: Show $A \Delta B$ on a Venn diagram. For $A = \{1, 2, 3\}$ and $B = \{3, 4, 5\}$, compute $A \Delta B$.

Cartesian product: of sets is a set consisting of ordered pairs (*tuples*), i.e.
$A \times B = \{(a, b) \text{ s.t. } a \in A, b \in B\}$.

$A = \{1, 2, 3\}$ and $B = \{3, 4, 5\}$.
$A \times B = \{(1, 3), (1, 4), (1, 5), (2, 3), (2, 4), (2, 5), (3, 3), (3, 4), (3, 5)\}$.

Similarly, $A \times B \times C = \{(a, b, c) \text{ s.t. } a \in A, b \in B, c \in C\}$.

Q. Is $A \times B = B \times A$? Ans: No. The order matters

Distributive Law: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

$z \in A \cap (B \cup C)$
iff $z \in A$ AND $z \in (B \cup C)$
iff $z \in A$ AND ($z \in B$ OR $z \in C$)
Use the distributivity of AND over OR, x AND (y OR z) = (x AND y) OR (x AND z).

iff ($z \in A$ AND $z \in B$) OR ($z \in A$ AND $z \in C$)
iff $z \in (A \cap B)$ OR $z \in (A \cap C)$
iff $z \in (A \cap B) \cup (A \cap C)$

Questions?

Functions

A function assigns an element of one set, called the *domain*, to an element of another set, called the *codomain* s.t. for every element in the domain, there is exactly one element in the codomain.

If A, B are sets then the function $f : A \rightarrow B$. Here A is the domain and B is the codomain.

If $a \in A$, and $b \in B$, and $f(a) = b$, we say the function f maps a to b, b is the value of f at argument a, f assigns the element b to a, b is the image of a, a is the preimage of b.

$A = \{a, b, c, \ldots z\}$, $B = \{1, 2, 3, \ldots 26\}$, then we can define a function $f : A \rightarrow B$ such that $f(a) = 1$, $f(b) = 2$. f thus assigns a number to each letter in the alphabet.

Consider $f : \mathbb{R} \rightarrow \mathbb{R}$ s.t. for $x \in \mathbb{R}$, $f(x) = x^2$. $f(2.5) = 6.25 \in \mathbb{R}$.

Functions

A function cannot assign different elements in the codomain to the same element in the domain. For example, if $f(a) = 1$ and $f(a) = 2$, the f is not a function.

A function that assigns a value to every element in the domain is called a *proper* function, while one that does not necessarily do so is called a *partial* function.

For $x \in \mathbb{R}$, $f(x) = 1/x^2$ is a partial function because no value is assigned to $x = 0$, since $1/0$ is undefined.

Q: For $x \in \mathbb{R}_+$, consider $f(x) = \sqrt{x}$. Is f a function? Ans: Yes

Q: For $x \in [-1, 1], y \in \mathbb{R}$, consider $g(x) = y$ s.t. $x^2 + y^2 = 1$. Is g a function? Ans: No

Q: For $x \in \{-1, 1\}, y \in \mathbb{R}$, consider $g(x) = y$ s.t. $x^2 + y^2 = 1$. Is g a function? Ans: Yes

Functions

Can define a function with a set as the argument. For a set $S \in D$,
$f(S) := \{x | \forall s \in S, x = f(s)\}$.

$A = \{a, b, c, \ldots z\}$, $B = \{1, 2, 3, \ldots 26\}$. $f : A \to B$ such that $f(a) = 1$, $f(b) = 2, \ldots$.
$f(\{e, f, z\}) = \{5, 6, 26\}$.

If D is the domain of f, then range$(f) := f(D) = f(\text{domain}(f))$.

Q: If $f : \mathbb{N} \to \mathbb{R}$, and $f(x) = x^2$. What is the domain and codomain of f? What is the range?

Ans: $\mathbb{N}$, $\mathbb{R}$, $\{0, 1, 4, 9, \ldots\}$

Q: Consider $f : \{0, 1\}^5 \to \mathbb{N}$ s.t. $f(x)$ counts the length of a left to right search of the bits in the binary string x until a 1 appears. $f(01000) = 2$.

What is $f(00001)$, $f(00000)$? Is f a total function? Ans: 5, undefined, No.

Surjective Functions

Surjective functions: If $f : A \to B$ is a surjective function, then for every $b \in B$, there exists an $a \in A$ s.t. $f(a) = b$.

For surjective functions, $|\#\text{arrows}| \geq |B|$.

Since each element of A is assigned at most one value, and some need not be assigned a value at all, $|\#\text{arrows}| \leq |A|$.

Hence, if f is a surjective function, then $|A| \geq |B|$.

$A = \{a, b, c, \ldots z, \alpha, \beta, \gamma, \ldots\}$, $B = \{1, 2, 3, \ldots 26\}$. $f : A \to B$ such that $f(a) = 1$, $f(b) = 2, \ldots$. f does not assign any value to the Greek letters. For every number in B, there is a letter in A. Hence, f is surjective. And $|A| > |B|$.

Injective & Bijective Functions

Injective functions: If f is an injective function, then $\forall a \in A$, there is a *unique* $b \in B$ s.t. $f(a) = b$.

Hence, $|\#\text{arrows}| = |A| \leq |B|$. Hence, if f is a injective function, then $|A| \leq |B|$.

$A = \{a, b, c, \ldots z\}$, $B = \{1, 2, 3, \ldots 26, 27, \ldots 100\}$. $f : A \to B$ such that $f(a) = 1$, $f(b) = 2, \ldots$. No element in A is assigned values $27, 28, \ldots$, and for every letter in A, there is a number in B. Hence, f is injective. And $|A| < |B|$.

Bijective functions: If f is a bijective function, then it is both surjective and injective, implying that $|A| = |B|$.

$A = \{a, b, c, \ldots z\}$, $B = \{1, 2, 3, \ldots 26\}$. $f : A \to B$ such that $f(a) = 1$, $f(b) = 2, \ldots$. Every element in A is assigned a value in B and for every element in B, there is a value in A that is mapped to it. f is bijective. And $|A| = |B|$.

Converse of the previous statements is also true.

- If $|A| \geq |B|$, then it's always possible to define a surjective function $f : A \to B$.
- If $|A| \leq |B|$, then it's always possible to define a injective function $f : A \to B$.
- If $|A| = |B|$, then it's always possible to define a bijective function $f : A \to B$.

Q: Recall that the Cartesian product of two sets $S = \{s_1, s_2, \ldots, s_m\}$, $T = \{t_1, t_2, \ldots, t_n\}$ is $S \times T := \{(s, t) | s \in S, t \in T\}$. Construct a bijective function $f : (S \times T) \to \{1, \ldots nm\}$, and prove that $|S \times T| = nm$.

Ans: $f(s_1, t_1) = 1$, $f(s_1, t_n) = n$, $f(s_2, t_1) = n + 1$, and so on. $f(s_i, t_j) = n(i-1) + j$. Since f is bijective, $|S \times T| = |\{1, \ldots nm\}| = nm$.

Questions?

Sequences

Examples: (a, b, a), (1,3,4), (4,3,1)

An element can appear twice. E.g. $(a, a, b) \neq (a, b)$.

The order of the elements does matter. E.g. $(a, b) \neq (b, a)$.

Q: What is the size of $(1, 2, 2, 3)$? What is the size of $\{1, 2, 2, 3\}$? Ans: 4, 3.

Sets and Sequences: The Cartesian product of sets $S \times T \times U$ is a set consisting of all sequences where the first component is drawn from S, the second component is drawn from T and the third from U. $S \times T \times U = \{(s, t, u) | s \in S, t \in T, u \in U\}$.

Q: For set $S = \{0, 1\}$, $S^3 = S \times S \times S$. Enumerate S. What is $|S^3|$?

Ans: $S^3 = \{(0, 0, 0), (0, 0, 1) \ldots (1, 1, 1)\}$, $|S^3| = 8$

Counting Sets - Example

Suppose we want to buy 10 donuts. There are 5 donut varieties – chocolate, lemon-filled, sugar, glazed, plain. Let A be the set of ways to select the 10 donuts. Each element of A is a potential selection. For example, 4 chocolate, 3 lemon, 0 sugar, 2 glazed and 1 plain.

Let's map each way to a string as follows: $\underbrace{0000}_{\text{chocolate}}\ \underbrace{000}_{\text{lemon}}\ \underbrace{\quad}_{\text{sugar}}\ \underbrace{00}_{\text{glazed}}\ \underbrace{0}_{\text{plain}}$.

Lets fix the ordering – chocolate, lemon, sugar, glazed and plain, and abstract this out further to get the sequence: 0000 1 000 1 1 00 1 0.

Hence, each way of choosing donuts is mapped to a binary sequence of length 14 with exactly 4 ones. Now, let B be all 14-bit sequences with exactly 4 ones. An element of B is 11110000000000.

Q: The above sequence corresponds to what donut order? Ans: All plain donuts.

For every way to select donuts, we have an equivalent sequence in B. And every sequence in B implies a unique way to select donuts. Hence, the above mapping from $A \to B$ is a bijective function.

Counting Sets - using a bijection

Hence, $|A| = |B|$, meaning that we have reduced the problem of counting the number of ways to select donuts to counting the number of 14-bit sequences with exactly 4 ones.

General result: The number of ways to choose n elements with k available varieties is equal to the number of $n + k - 1$-bit binary sequences with exactly $k - 1$ ones.

Q: There are 2 donut varieties – chocolate and lemon-filled. Suppose we want to buy only 2 donuts. Use the above result to count the number of ways in which we can select the donuts? What are these ways?

Ans: Since $n = 2$, $k = 2$, we want to count the sequences with exactly 1 one in 3-bit sequences. $\{(0, 0, 1), (1, 0, 0), (0, 1, 0)\}$.

Q: In the above example, I want at least one chocolate donut. What are the types of acceptable 3-bit sequences with this criterion? How many ways can we do this?

Ans: We want to count the number of 3-bit sequences that start with zero and have exactly 1 one in them. So $\{(0, 1, 0), (0, 0, 1)\}$.

Counting Sequences - using the product rule

Suppose the university offers Math courses (denoted by the set M), CS courses (set C) and Statistics courses (set S). We need to pick one course from each subject – Math, CS and Statistics. What is the number of ways we can select we can select the 3 courses?

The above problem is equivalent to counting the number of sequences of the form (m, c, s) that maps to choose the Math course m, CS course c and Stats course s.

Recall that the product of sets $M \times C \times S$ is a set consisting of all sequences where the first component is drawn from M, the second component is drawn from C and the third from S. $M \times C \times S = \{(m, c, s) | m \in M, c \in C, s \in S\}$. Hence, counting the number of sequences is equivalent to computing $|M \times C \times S|$.

Product Rule: $|M \times C \times S| = |M| \times |C| \times |S|$.

Using the above equivalence, the number of sequences and hence, the number of ways to select the 3 courses is $|M| \times |C| \times |S|$.

Counting Sequences - Example

What is the number of length n-passwords that can be generated if each character in the password is allowed to be lower-case letter?

Each possible sequence is of the form $(a, b, d, \ldots,)$ where the first element in the sequence can be selected from the $\{a, b, \ldots z\}$ set. Similar reasoning holds for each element.

Using the equivalence between sequences and products of sets, counting the number of such sequences is equivalent to computing $|\{a, b, \ldots z\} \times \{a, b, \ldots z\} \times \{\text{a,b,} \ldots z\} \ldots|$.

Using the product rule, $|\{a, b, \ldots z\} \times \{a, b, \ldots z\} \times \{a, b, \ldots z\} \ldots| = |\{a, b, \ldots z\}| \times |\{a, b, \ldots z\}| \times \ldots = 26^n$.

Counting Sets - using the sum rule

Let R be the set of rainy days, S be the set of snowy days and H be the set of really hot days in 2022. A bad day can be either rainy, snowy or really hot. What is the number of good days?

Let B be the set of bad days. $B = R \cup S \cup H$, and we want to estimate $|\bar{B}|$. $|D| = 365$.
$|\bar{B}| = |D| - |B| = 365 - |B| = 365 - |R \cup S \cup H|$.

Since the sets R, S and H are disjoint, $|R \cup S \cup H| = |R| + |S| + |H|$, and hence the number of good days $= 365 - |R| - |S| - |H|$.

Sum rule: If $A_1, A_2 \ldots A_m$ are disjoint sets, then, $|A_1 \cup A_2 \cup \ldots \cup A_m| = \sum_{i=1}^{m} |A_i|$.

Counting Sets - Example

What is the number of passwords that can be generated if the (i) first character is only allowed to be a lower-case letter, (ii) each subsequent character in the password is allowed to be lower-case letter or digit $(0-9)$ and (iii) the length of the password is required to be between 6-8 characters?

Let $L = \{a, b, \dots z\}$ and $D = \{0, 1, 2, \dots\}$. Using the equivalence between sequences and products of sets, the set of passwords of length 6 is given by $P_6 = L \times (L \cup D)^5$. Using the product rule, $|P_6| = |L| \times (|L \cup D|)^5 = |L| \times (|L| + |D|)^5$.

Since the total set of passwords are $P = P_6 \cup P_7 \cup P_8$, $|P| = |P_6| + |P_7| + |P_8| = |L| \times \left[(|L| + |D|)^5(1 + (|L| + |D|) + (|L| + |D|)^2)\right] = 26 \times 36^5 \times [1 + 36 + 1296]$.

Questions?