CMPT 210: Probability and Computing

Lecture 1

Sharan Vaswani

January 5, 2023

Course Information

- **Instructor**: Sharan Vaswani (TASC-1 8221) Email: sharan_vaswani@sfu.ca
- **Office Hours**: Thursday 2.30 pm - 3.30 pm (TASC-1 8221)
- **Teaching Assistant**: Anh Dang. Email: anh_dang@sfu.ca
- **Tutorials**: (From 16 Jan) Monday (1:30 pm - 2:20 pm, 3.30 pm - 4.20 pm) in BLU 10921
- **Course Webpage**: https://vaswanis.github.io/210-W23
- **Piazza**: https://piazza.com/sfu.ca/spring2023/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: Permutations, Binomial coefficients, Inclusion-Exclusion
- Probability theory: Independence, Conditional probability, Bayes' Theorem
- Probability theory: Random variables, Expectation, Variance
- Discrete distributions: Bernoulli, Binomial and Geometric, Joint distributions
- Tail inequalities: Markov's Inequality, Chebyshev's Inequality, Chernoff Bound
- Applications: Verifying matrix multiplication, Max-Cut, Machine Learning, Randomized QuickSort, AB Testing
- Continuous distributions (Introduction): Normal Distribution, Central Limit Theorem

Primary Resources:

- Mathematics for Computer Science (Meyer, Lehman, Leighton): `https://people.csail.mit.edu/meyer/mcs.pdf`
- Introduction to Probability and Statistics for Engineers and Scientists (Ross).

Course Information

Grading:

- 5 Assignments ($5 \times 10\% = 50\%$)
- 1 Mid-Term ($1 \times 15\% = 15\%$) (17 February)
- 1 Final Exam ($1 \times 35\% = 35\%$) (TBD)

- Each assignment is due in 1 week (on Fridays).
- For some flexibility, each student is allowed 1 late-submission and can submit the assignment in the tutorial session (the Monday after).
- Solutions will be released on Monday evenings after the tutorial, and no late submissions are allowed after that.
- If you miss the mid-term (for 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 definition: 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 $|A|$?

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 $\{1, 4, 2\} \subseteq \{2, 4, 1\}$
Q: Is $\mathbb{N} \subset \mathbb{Z}$? Is $\mathbb{C} \subset \mathbb{R}$?
Q: What is $|\emptyset|$?

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 Operations

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 $\overline{A \cap B}$, $(B \backslash A) \cup (A \backslash B)$.

Power set of A is the set of all subsets of A. If $A = \{a, b, c\}$, then $\mathrm{Pow}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$.

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.
$A \times B = \{(a, b) \text{ s.t. } a \in A, b \in B\}$. If $A = \{1, 2, 3\}$ and $B = \{3, 4, 5\}$.
$A \times B = \{(1, 3), (1, 4), (1, 5), (2, 3), (2, 4), (2, 5), (3, 3), (3, 4), (3, 5)\}$.

If sets are 1-dimensional objects, Cartesian product of 2 sets can be thought of as 2-dimensional.

Q. Is $A \times B = B \times A$?

In general, $A_1 \times A_2 \times \ldots \times A_k = \{(a_1, a_2, \ldots, a_k) | a_1 \in A_1, a_2 \in A_2, \ldots, a_k \in A_k\}$ where $(a_1, a_2, \ldots, a_k)$ is referred to as a k-tuple.

Laws of Set Theory

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, for binary literals $w, x, y \in \{0, 1\}$, x AND (y OR w) = (x AND y) OR (x AND w). For $x := z \in A$, $y := z \in B$, $w := z \in C$,

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 at most one element in the codomain.

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

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, 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 $x \in \mathbb{R}$, $f(x) = x^2$. $f(2.5) = 6.25 \in \mathbb{R}$.

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.

Functions

A function that assigns a value to every element in the domain is called a *total* 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: Consider $f : \mathbb{R}_+ \to \mathbb{R}$ such that $f(x) = x$. Is f a function?

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?

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?

Functions

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

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

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?

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?

Surjective Functions

Surjective functions: $f : A \to B$ is a surjective function iff for every $b \in B$, there exists an $a \in A$ s.t. $f(a) = b$. $f : \mathbb{R} \to \mathbb{R}$ such that $f(x) = x + 1$ is a surjective function.

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: $f : A \to B$ is an injective function iff $\forall a \in A$, there is a *unique* $b \in B$ s.t. $f(a) = b$. If f is injective and $f(a) = f(b)$, then it implies that $a = b$.

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 unique number in B. Hence, f is injective, and $|A| < |B|$.

Bijective functions: f is a bijective function iff 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 unique value in B and for every element in B, there is a value in A that is mapped to it. f is bijective, and $|A| = |B|$.

Functions

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 $|S \times T| = nm$.

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 $\{1, 2, 2, 3\}$? .

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^3. What is $|S^3|$?

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: $\underbrace{0000}_{\text{chocolate}}\ \underbrace{000}_{\text{lemon}}\ \underbrace{}_{\text{sugar}}\ \underbrace{00}_{\text{glazed}}\ \underbrace{0}_{\text{plain}}$.

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?

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 $A \rightarrow B$ 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?

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?

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, i.e. $M \times C \times S = \{(m, c, s) | m \in M, c \in C, s \in S\}$. 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 password is of the form $(a, b, d, \ldots,)$ where each element in the sequence can be selected from the $\{a, b, \ldots z\}$ set.

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

Questions?