

# CMPT 210: Probability and Computing

## Lecture 1

---

Sharan Vaswani

September 5, 2024

- **Instructor:** Sharan Vaswani (TASC-1 8221) Email: [sharan\\_vaswani@sfu.ca](mailto:sharan_vaswani@sfu.ca)
- **Instructor Office Hours:** Tuesday 3 pm - 4 pm (TASC-1 8221)
- **Teaching Assistants:** Kaixuan Hu, Dingdong Yang, Haidan Liu, Harsimran Singh
- **Tutorials** (beginning September 17):
  - D100: Friday (11.30 am - 12.20 am, 12:30 pm - 1.20 pm) (WMC 2533 & WMC3511)
  - D200: Tuesday (4.30 pm - 5.20 pm, 5:30 pm - 6.20 pm) (WMC 2501 & AQ 5035)
- **Course Webpage:** <https://vaswanis.github.io/210-F24.html>
- **Piazza:** <https://piazza.com/sfu.ca/fall2024/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

## 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).

## Grading:

- 4 Assignments (45%)
- 1 Mid-Term (20%) (Tentatively 22 October)
- 1 Final Exam (35%) (TBD)
  
- Each assignment is due in 1 week via Coursys.
- For some flexibility, each student is allowed 1 late-submission and can submit the assignment the following Tuesday/Thursday.
- If you miss the mid-term (for a well-justified reason), we will reassign weight to the final.
- If you miss the final, there will be a make-up exam.

Questions?

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

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

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.  $A = \{a, b\} = \{b, a\}$ .

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

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

**Membership:**  $\text{red} \in C$ ,  $\text{brown} \notin C$ .

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

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

# Common Sets

- $\emptyset$ : Empty Set
- $\mathbb{N}$ : Set of nonnegative integers  $\{0, 1, 2, \dots\}$
- $\mathbb{Z}$ : Set of integers  $\{-2, -1, 0, 1, 2, \dots\}$
- $\mathbb{Q}$ : Set of rational numbers that can be expressed as  $p/q$  where  $p, q \in \mathbb{Z}$  and  $q \neq 0$ .  
 $\{-10.1, -1.2, 0, 5.5, 15, \dots\}$
- $\mathbb{R}$ : 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  $|\emptyset|$ ?

**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  $A \setminus B = A - B = \{1, 2\}$ .  $B \setminus A = B - A = \{4, 5\}$ .

**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  $\bar{A} = \{0, 4, 5, 6, \dots\}$ .

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

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

**Power set** of  $A$  is the set of all subsets of  $A$ . If  $A = \{a, b, c\}$ , then

$$\text{Pow}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

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

**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  $b$ .

$A = \{a, b, c, \dots, z\}$ ,  $B = \{1, 2, 3, \dots, 26\}$ , 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.

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  $f : \mathbb{R}_+ \rightarrow \mathbb{R}$  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?

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

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

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

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

**Q:** Consider  $f : \{0, 1\}^5 \rightarrow \mathbb{N}$  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:**  $f : A \rightarrow B$  is a surjective function iff for every  $b \in B$ , there exists an  $a \in A$  s.t.  $f(a) = b$ .  $f : \mathbb{R} \rightarrow \mathbb{R}$  such that  $f(x) = x + 1$  is a surjective function.

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

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

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

$A = \{a, b, c, \dots, z, \alpha, \beta, \gamma, \dots\}$ ,  $B = \{1, 2, 3, \dots, 26\}$ .  $f : A \rightarrow B$  such that  $f(a) = 1$ ,  $f(b) = 2, \dots$ .  $f$  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:**  $f : A \rightarrow B$  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  $|A| \leq |B|$ .

$A = \{a, b, c, \dots, z\}$ ,  $B = \{1, 2, 3, \dots, 26, 27, \dots, 100\}$ .  $f : A \rightarrow B$  such that  $f(a) = 1$ ,  $f(b) = 2, \dots$ . No element in  $A$  is assigned values  $27, 28, \dots$ , 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  $|A| = |B|$ .

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

Converse of the previous statements is also true.

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

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

**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  $|S^3|$ ?

Questions?