Course Notes

CSCA67 - Discrete Mathematics

Instructors:

	Dr. Anna Bretscher	**Dr. Richard Pancer**
Email:	bretscher@utsc.utoronto.ca	pancer@utsc.utoronto.ca
Office:	IC493	IC490
Office Hours:	Monday 12:10 - 1:30 Wednesday 1:10 - 2:00 Friday 1:10 - 2:00 (will change after week 6)	Monday 11:10 - 12:30 Friday 1:30 - 3:00

1 Propositions, Implications

Definitions:

A **proposition** is a statement that evaluates to True or False. In computer science, its often referred to as a **Boolean expression**.

A **compound roposition** is a proposition statementt that involves multiple propositions joined by connectives. It takes multiple truth values as input and returns a single truth value as output.

A **connective** corresponds to English conjunctions such as "and", "or", "not" etc.

Basic connectives and truth tables:

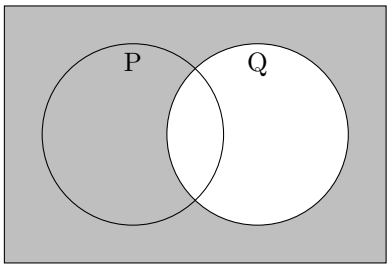
Symbol	Meaning
$\wedge$	"AND"
$\vee$	"OR"
$\rightarrow$	"IF...THEN"
$\leftrightarrow$	"IF AND ONLY IF"
$\neg$	"NOT"

P	Q	$P \wedge Q$	$P \vee Q$	$P \rightarrow Q$	$P \leftrightarrow Q$
T	T	T	T	T	T
T	F	F	T	F	F
F	T	F	T	T	F
F	F	F	F	T	T

Implication:

Different ways of writing $P \rightarrow Q$:

1. If P then Q
2. If P, Q
3. Q, if P
4. P only if Q
5. P is sufficient for Q
6. Q is neccesary for P
7. If not Q, then not P
8. Not P or Q



Logical Equivalences:

Commutative	$p \wedge q \iff q \wedge p$	$p \vee q \iff q \vee p$
Associative	$(p \wedge q) \wedge r \iff p \wedge (q \wedge r)$	$(p \vee q) \vee r \iff p \vee (q \vee r)$
Distributive	$p \wedge (q \vee r) \iff (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \iff (p \vee q) \wedge (p \vee r)$
Identity	$p \wedge T \iff p$	$p \vee F \iff p$
Negation	$p \vee \neg p \iff T$	$p \wedge \neg p \iff F$
Double Negative	$\neg(\neg p) \iff p$	
Idempotent	$p \wedge p \iff p$	$p \vee p \iff p$
Universal Bound	$p \vee T \iff T$	$p \wedge F \iff F$
De Morgan's	$\neg(p \wedge q) \iff (\neg p) \vee (\neg q)$	$\neg(p \vee q) \iff (\neg p) \wedge (\neg q)$
Absorption	$p \vee (p \wedge q) \iff p$	$p \wedge (p \vee q) \iff p$
Conditional or ($\rightarrow$) Law	$(p \rightarrow q) \iff (\neg p \vee q)$	$\neg(p \rightarrow q) \iff (p \wedge \neg q)$
Biconditional	$(p \leftrightarrow q) \iff (p \rightarrow q) \wedge (q \rightarrow p)$	

Order of Operations:

1. NOT($\neg$) 2. AND($\wedge$) 3. OR($\vee$) 4. Quantifiers($\forall/\exists$) 5. ($\rightarrow$ / $\leftrightarrow$)

2 Predicates and Quantifiers

Forall:	$\forall$
There exists:	$\exists$
Negations:	
$\neg\forall = \exists$	$\neg\exists = \forall$

Prove statement in the form of $\exists x \in S, \ni: P(x)$
We simply need to find **one** value of x in the set S, that makes $P(x)$ true.
One value is enough.

Example:
There exists an integer n, such that n^2 is even.
$\exists n \in \mathbb{Z}, \ni: n^2 \in 2\mathbb{Z}$
Let $n = 2$, then $(2)^2 = 4$ which is an even number

Prove statemnet in the form of $\forall x \in S, \ni: P(x)$
This means we must use techniques such as algebraic manipulation to show that:
$P(x)$ holds for every arbitrary $x \in S$

Example:
Forall integers n, if n is even, then n^2 is even.
$\forall n \in \mathbb{Z}, n = 2k, k \in \mathbb{Z} \rightarrow n^2 = 2z, z \in \mathbb{Z}$
Let $n = 2k, k \in \mathbb{Z}$
then $n^2 = (2k)^2 = 4k^2$ which is an even number.
Therefore: Forall integers n, if n is even, then n^2 is even. QED

2.1 Modulus

$$10 \textbf{ mod } 3 = 1$$

The modulus or "mod" operator means the remainder when we divide two numbers.
Congruent mod means that two numbers have the same remainder when divided by one number.

$$10 \equiv_3 7 \Leftrightarrow 10 \bmod 3 = 7 \bmod 3$$

2.2 Fundamental Theorem of Arithmetic

The **Fundamental Theorem of Arithmetic** states that any integer greater than 1 is either a **prime** number itself, or can be represented as the unique product of prime numbers.
For example:

$$\begin{aligned} 16 &= 2^4 \\ 18 &= 2^1 \cdot 3^2 \\ 21 &= 2^0 \cdot 3^1 \cdot 5^0 \cdot 7^1 \end{aligned}$$

Numbers that can be written as the unique product of primes are called **Composite Numbers**.
Reminder: a **prime number** is an number that can only be divided evenly by 1 and the number itself.

3 Basic Proof Strategies

To prove in the form of $P \to Q$:

Direct Proof: Assume P is true then prove Q

This form works because if we recall the truth table for $P \to Q$,
When P is true, Q must be true for the statement to evaluate to true.

Proof by Contrapositve: Assume $\neg Q$ is true then prove $\neg P$

This form works because the contrapositive is logically equivalent to the original,
$P \to Q \equiv \neg Q \to \neg P$

Proof by Contradiction: Assume $\neg(\neg(P \to Q)) \equiv P \wedge \neg Q$

Then we must derive some sort of contradiction.
Once we arrive at the contradiction, that means one of our assumptions cannot be correct.
for example if $\neg Q$ is false, that means Q is true.

Proof by Cases/Exhaustion: $X \vee Y \to Q$ Show $X \to Q \wedge Y \to Q$
Example:
$x \in \mathbb{Z} \to x^2 + x + 1 \in 2\mathbb{Z} + 1$ ($x^2 + x$ is odd)

Case 1: x is odd
$x = 2k + 1$
$(2k + 1)^2 + (2k + 1) + 1$
$= 4k^2 + 6k + 3$
$= 2(2k^2 + 3) + 3$ case holds when x is odd.

Case 2: x is even
$x = 2k$
$(2k^2) + 2k + 1$
$= 4k^2 + 2k + 1$
$= 2(2k^2 + k) + 1$ case holds when x is even.
Since we have proven both case are indepdently even, we can conclude $\forall x \in \mathbb{Z}, x^2 + x + 1 \in 2\mathbb{Z} + 1$

Some Definitions:

Theorem: A statement that has already been proved.

Axiom: A statement that is self evidently true.

Identiy: An equation that is true for all values of an arbitrary variable.

Proof: A mathematical argument demonstrating the truth of a proposition.

Tautology: A propositional logic formula that always evaluates to True. $(A \vee \neg A)$ - (I'm hungry or I'm not hungry)

Rational Number: A number that can be represented as the fraction of two relatively prime integers.

$$A \in \mathbb{Q} \to A = \frac{m}{n}, n \neq 0, m, n \in \mathbb{Z}, gcd(m, n) = 1$$

Logic in a nutshell

Statement	Ways to Prove it	Ways to Use it	How to Negate it
p	• Prove that p is true. • Assume p is false, and derive a contradiction.	• p is true. • If p is false, you have a contradiction.	not p
p and q	• Prove p, and then prove q.	• p is true. • q is true.	(not p) or (not q)
p or q	• Assume p is false, and deduce that q is true. • Assume q is false, and deduce that p is true. • Prove that p is true. • Prove that q is true.	• If $p \Rightarrow r$ and $q \Rightarrow r$ then r is true. • If p is false, then q is true. • If q is false, then p is true.	(not p) and (not q)
$p \Rightarrow q$	• Assume p is true, and deduce that q is true. • Assume q is false, and deduce that p is false.	• If p is true, then q is true. • If q is false, then p is false.	p and (not q)
$p \iff q$	• Prove $p \Rightarrow q$, and then prove $q \Rightarrow p$. • Prove p and q. • Prove (not p) and (not q).	• Statements p and q are interchangeable.	(p and (not q)) or ((not p) and q)
$(\exists x \in S)\ P(x)$	• Find an x in S for which $P(x)$ is true.	• Say "let x be an element of S such that $P(x)$ is true."	$(\forall x \in S)$ not $P(x)$
$(\forall x \in S)\ P(x)$	• Say "let x be any element of S." Prove that $P(x)$ is true.	• If $x \in S$, then $P(x)$ is true. • If $P(x)$ is false, then $x \notin S$.	$(\exists x \in S)$ not $P(x)$

Graph from Introduction to mathematical arguments - by Michael Hutchings

4 Proof of Irrationality

4.1 Approach 1 - Fundamental Theorem of Arithmetic

Prove that $\sqrt{2}$ is irrational.

Assume the contrary that $\sqrt{2}$ is rational.
Then by the definition of rational numbers, $\sqrt{2} = \frac{m}{n}, \ni: m, n \in \mathbb{Z}, gcd(m,n) = 1, n \neq 0$

$$\sqrt{2} = \frac{m}{n}$$
$$n\sqrt{2} = m$$
$$2n^2 = m^2$$
$$m = x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot x_3^{\alpha_3} \cdot \cdots \cdot x_n^{\alpha_n} \qquad n = {y_1}_1^{\beta} \cdot y_2^{\beta_2} \cdot y_3^{\beta_3} \cdot \cdots \cdot y_n^{\beta_n}$$

Each x, y are primes by the fundamental theorem of arithmetic.

$$m^2 = (x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot x_3^{\alpha_3} \cdot \cdots \cdot x_n^{\alpha_n})(x_1^{\alpha_1} \cdot x_2^{\alpha_2} \cdot x_3^{\alpha_3} \cdot \cdots \cdot x_n^{\alpha_n})$$

This means that m^2 has $2n$ possible factors.

$$2n^2 = 2({y_1}_1^{\beta} \cdot y_2^{\beta_2} \cdot y_3^{\beta_3} \cdot \cdots \cdot y_n^{\beta_n})({y_1}_1^{\beta} \cdot y_2^{\beta_2} \cdot y_3^{\beta_3} \cdot \cdots \cdot y_n^{\beta_n})$$

This means that n^2 has $2n$ possible factors plus one factor 2.

as m^2 has an even number of prime factors, $2n^2$ will have an odd number of prime factors, contradicting the fundamental theorem.

$\therefore \sqrt{2} \in \mathbb{I}$ by contradiction. QED

4.2 Approach 2 - Definition of a Rational Number

Prove that $\sqrt{2}$ is irrational.

Assume the contrary that $\sqrt{2}$ is rational.
Then by the definition of rational numbers, $\sqrt{2} = \frac{m}{n}, \ni: m, n \in \mathbb{Z}, gcd(m,n) = 1, n \neq 0$

$gcd(m,n)$ means that m, n MUST be relative prime.

$$\sqrt{2} = \frac{m}{n}$$
$$n\sqrt{2} = m$$
$$2n^2 = m^2$$
$$2n^2 = m^2 \Rightarrow m^2 \in 2\mathbb{Z} \Rightarrow m \cdot m \in 2\mathbb{Z}$$

The previousline showed that m is even, so now we can substitute m with any arbitrary even number $2k$.

$$m = (2k), k \in \mathbb{Z}$$
$$2n^2 = (2k^2)$$
$$2n^2 = 4k^2$$
$$n^2 = 2k^2$$
$$n^2 \in 2\mathbb{Z} \Rightarrow n \in 2\mathbb{Z}$$
$$m, n \in 2\mathbb{Z} \Rightarrow gcd(m,n) \neq 1$$

Since m, n are both even, they cannot be relatively prime, $\therefore \sqrt{2} \in \mathbb{I}$ by contradiction. QED

5 Induction

Simple Induction Format:
Suppose we need to prove $P(n)$ for all natural numbers.

1. State the Predicates
$P(n) : \ldots$

2. Base case
Prove that $P(n)$ holds when n is the smallest possible natural number.
$P(0) : \ldots$ is True.

3. Inductive Hypothesis
Assume that $P(k)$ holds for any arbitrary k
$P(k) : \ldots$ is True.

4. Inductive Step
Prove that $P(k) \rightarrow P(k+1)$
Assume $P(k)$ then show $P(k+1)$

Example: Prove $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$

Stating the Predicate: $P(n) : \sum_{i=0}^{n} i = \frac{n(n+1)}{2}, \forall n \in \mathbb{N}$

Base case: $n = 0 : \sum_{i=0}^{0} i = 0 \quad \frac{0(0+1)}{2} = 0$

Inductive Hypothesis: Assume for any arbitrary $k \geq 0$, $P(k)$ holds.
$P(k) = \sum_{i=0}^{k} k = \frac{k(k+1)}{2}$
Inductive Step: Prove $P(k) \rightarrow P(k+1)$

$P(k+1) = \sum_{i=0}^{k+1} i = 1 + 2 + 3 \cdots + k + (k+1)$

$P(k+1) = \frac{k(k+1)}{2} + (k+1)$ **by Inductive Hypothesis**

$P(k+1) = \frac{k(k+1)+2(k+1)}{2}$
$P(k+1) = \frac{(k+1)(k+2)}{2}$
Conclusion:
$\therefore P(k) \rightarrow P(k+1)$
$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}, \forall n \in \mathbb{N}$

6 Pigeonhole Principle

Core Principle: There exists n pigeons and m pigeonholes, if $n > m$, there must be atleast one pigeonhole with atleast two pigeons.

Example: Prove that if 7 distinct numbers are selected from $\{1, 2, \ldots 11\}$, then some two will add to 12.

Pigeons: 7 distinct numbers

Pigeonholes: 6 **sets** of numbers that add up to 12.

$$\{1, 11\}, \{2, 10\}, \{3, 9\}, \{4, 8\}, \{5, 7\}, \{6\}$$

Note: If we select 7 numbers from a set of 6, we will be forced to select atleast 2 of the numbers from the same set.

$\therefore$ if 7 distinct numbers are selected from $\{1, 2, \ldots 11\}$, then atleast two will add up to 12. QED

7 Proof Samples

7.1 Euclid's Proof for Infinite Primes

Assume to the contrary that there are a finite number of primes,
then let this be the complete set of primes: $p_1, p_2, p_3 \dots p_n$

---

let $A = (p_1 \cdot p_2 \cdot p_3 \cdot p_4 \dots, \cdot p_n) + 1$
A is not divisible by any known primes as it always leaves a remainder of 1.
so either A is a prime number itself, or A has a unique prime factor that is not in the existing list.

Contradictions:
if A is a prime number, then p_n is not the greatest prime.
if A is a composite number, then $p_1, p_2, p_3 \dots p_n$ does not contain all the primes.
Therefore, there must be an infinite number of primes.

QED

7.2 Arithmetic mean and Geometric mean

Defintion. The arithmetic mean of a_1, a_2:

$$\frac{a_1 + a_2}{2}$$

Definition. The geometric mean of a_1, a_2:

$$\sqrt{a_1 \cdot a_2}$$

Prove that: $\forall a_1, a_2 \in \mathbb{Z}^+, \frac{a_1 + a_2}{2} \geq \sqrt{a_1 \cdot a_2}$

$$\frac{a_1 + a_2}{2} \geq \sqrt{a_1 \cdot a_2}$$
$$(\frac{a_1 + a_2}{2})^2 \geq a_1 \cdot a_2$$
$$\frac{{a_1}^2 + 2(a_1 \cdot a_2) + {a_2}^2}{4} \geq a_1 \cdot a_2$$
$${a_1}^2 + 2(a_1 \cdot a_2) + {a_2}^2 \geq 4(a_1 \cdot a_2)$$
$${a_1}^2 + 2(a_1 \cdot a_2) + {a_2}^2 - 4(a_1 \cdot a_2) \geq 0$$
$${a_1}^2 - 2(a_1 \cdot a_2) + {a_2}^2 \geq 0$$
$$(a_1 - a_2)^2 \geq 0$$

QED

8 Strong Induction

Strong Induction Format:

Suppose we need to prove $P(n)$ for all natural numbers.

1. State the Predicates

$P(n) : \ldots$

2. Base cases

Unlike Simple Induction, Strong Induction requires multiple base cases to be proven, starting with the smallest value for n.

Important note: Dr.Pancer says natural numbers start at 1.

3. Inductive Hypothesis

Assume that $P(k)$ holds for any arbitrary k

$P(k) : \ldots$ is True.

4. Inductive Step

Prove that $P(k) \rightarrow P(k+1)$

Assume $P(k)$ then show $P(k+1)$

A more formal way to write the Inductive Step for Strong Induction:

$P(1) \wedge P(2) \wedge P(3) \cdots \wedge \ldots P(k) \rightarrow P(k+1)$, where $P(1), P(2), P(3)$ were your base cases.

You may have to use your **Inductive Hypothesis** more than once.

Example on next page

Example: An alien race of hopkinsville goblins only have 4-cent and 5-cent coins in their currency. Prove that any amount of money greater than 12 cents, can be made using only 4-cent and 5-cent coins.

1. Stating the Predicates
$P(n) : \forall n \in \mathbb{N}, \ni: n \geq 12, n = 4a + 5b$

2. Base cases
$P(12) = 4(3) + 5(0)$
$P(13) = 4(2) + 5(1)$
$P(14) = 4(1) + 5(2)$
$P(15) = 4(0) + 5(3)$

3. Inductive Hypothesis
Suppose that $P(k)$, for any arbitrary k where $k \in [15, n)$
$P(k) : k = 4a + 5b$

4. Inductive Step
$P(k) \rightarrow P(k + 4)$
$k = 4a + 5b$ Suppose $P(k)$ by **Inductive Hypothesis**
$k + 4 = 4a + 5b + 4$
$k + 4 = 4(a + 1) + 5b$
Since k is arbitrary, $\forall n \in \mathbb{N}, P(n)$

Therefore, any amount of money greater than 12 cents, can be made using 4-cent and 5-cent coins by strong induction. QED

9 The Sum Rule

When counting, we need to be able to determine whether to sum or multiply the number of objects.

The Sum Rule. If an operation can be performed in n different ways, each having x_1 possible outcomes, then the total number of outcomes possible is:

$$\sum_{i=1}^{n} x_i = x_1 + x_2 \cdots + x_n$$

Example. Ordering pizza. Suppose a pizza shop offers 5 types of toppings and one has the choice of 3 topping, 2 topping or 1 topping.

Duplicate toppings are not allowed.

Order of toppings does not matter.

Determine how many different pizzas can be orderd.

Note: On the final, if a problem feels like it's unspecified, you are allowed to make your own assumptions, and answer them according to assumptions.

If you are right, you will not be penalized.

Number of Toppings	Number of Pizza Choices (x_i)
1	5
2	$\frac{5 \cdot 4}{2!}$
3	$\frac{5 \cdot 4 \cdot 3}{3!}$

10 The Product Rule

The Product Rule. Suppose an operation takes k steps and that:

- The first step can be performed x_1 ways.
- The second step can be performed in x_2 ways.

Then the Whole operation can be performed in:

$$\prod_{i=1}^{k} x_1 = x_1 \cdot x_2 \cdot \cdots \cdot x_k$$

Example. Given 4 cities A, B, C and D. Suppose:

- 5 routes between A and B
- 3 routes between B and C and
- 4 routes between C and D

How many different routes are there from A to D?

Number of AD routes $= 5 \cdot 3 \cdot 4 = 60$

Q. We have seen two different counting scenarios - creating a Google password and ordering apair of pizzas. Which one involved the sum rule and which one involved the product rule?

A. The password problem involved the product rule, the pizza problem used both.

11 Arrangement

An arrangement is a grouping of objects. There are two types of arrangements:

Definition. A **Permutation** is an arrangement in which order matters.

Definition. A **Combination** is an arrangement in which order does not matter.

12 Permutations

Definition. An r-permutation of n distincts objects is an orderd arrangement of r of the n objects. We use the notation $P(n, r)$

The formula is derived as $n \cdot (n-1)_1 \cdot (n-2)_2 \cdot \cdots \cdot (n-r+1)_r$

$P(11, 3) = 11 \cdot 10 \cdot 9$, $11 - 3 + 1$, $n = 11, r = 3$

Q. In terms of factorials, how can we rewrite this formula?

A. $P(n, r) = \dfrac{n!}{(n-r)!}$

13 Combinations

Defintion. An r-cominbation of n distinct objects is an unorderd selection, or a subset of r of the n objects.

We can think of combinations in terms of permutations.

Q. Given $P(n.r)$, the number of r-permutations of n objects, how can we derive the number of $C(n, r)$ of r-combinations of n objects?

A. $C(n, r) = \dfrac{P(n, r)}{r!} = \dfrac{n!}{(n-r)! \cdot sr!}$

$C(n, r) = {C_r}^n \equiv n(C_r) \equiv \binom{n}{r}$

Example. In Poker each player has 5 cards. A standard deck has 52 cards. How many 5-card hands are possible?

$C(52,5) = \binom{52}{5} = \frac{52!}{47! \cdot 5!} = 2,598,960$

A flush is when all 5 cards have the same suit. If there are 4 suits, i.e., 13 cards per suit, how many ways are there to obtain a flush?

$4 \cdot C(13,5) = 4 \cdot \frac{13!}{8! \cdot 5!} = 5148$

Possiblity of a flush $= \frac{5148}{2,598,960} \approx 0.2\%$

Q. Should flushes happen very often?

A. No.

Exercise. How many different 8-digit binary sequences are there with six 1s and two 0s?

for example: 11011101

8 bins must be filled in with six 1s and two 0s.

We should consider only filling in the 0s, as the 1s should fill in the rest of the space accordingly.

This is a combination:

$C(8,2) = C(8,6) = \frac{8!}{2! \cdot 6!}$

Bin technique - Pancer

14 Pascal's Triangle

Blaise Pascal [1623-1662] was a French mathematician, physicist, inventor, writer and philosopher

- As a teenager, he invented the mechanical calculator.
- He collaborated with Pierre de Fermat in Probability Theory influencing modern economics and social sciences.
- Invented Pascals Triangle in his Treatise on the Arithmetic Triangle.

$n=0$				1			
$n=1$			1		1		
$n=2$		1		2		1	
$n=3$	1		3		3		1
$n=4$		1		4		6		4		1	
$n=5$	1		5		10		10		5		1
$n=6$	1	6		15		20		15		6		1
	0	1		2		3		4		5		6

Q. What do you notice about each number? How is it related to pizza and toppings?

A. $(n,r)^{th}$ element = C(n,r)

Q. How is Pascals Triangle related to binomial expansion? I.e., how is it related to the coefficients of the polynomials found by expanding $(a+b)^n$?

A.
$(a+b)^1 = 1a + 1b$
$(a+b)^2 = 1a^2 + 2ab + 1b^2$
$(a+b)^3 = 1a^3 + 3a^2b + 3b^2a + 1b^3$
...

Q. What do each line sum to?

A. $1(2^0), 2(2^1), 4(2^2), 8(2^3) \ldots$ powers of 2

Q. Read each line as a number (catenate). If a number has two digits carry the tens digit to the left and add. What do these numbers represent?

A. $1, 11, 121, 1331, 14541 \ldots$ powers of 11.

Q. Colour all the odd numbers. What does this remind you of?

A. A well known repeating pattern, the Sierpinkski Triangle.

Q. What series of numbers do you get by adding up the numbers of the same colour which are on a stretched diagonal?

A. The Fibonacci sequence

Pascal was not the first to discover the triangle of binomial coefficients but was given credit because of how he related it to his work with probability and expectation.

15 Probability

The definition we will use was first defined by the French mathematician Pierre-Simon Laplace. He is famous for his work in astronomy, statistics and physics:

- Laplace tranform, Laplaces equation

- First to postulate the existence of black holes

- inductive reasoning based on probability, today called Bayesian probability which plays a large role in artificial intelligence.

Definition. An experiment is a clearly defined procedure that results in one of a possible set of outcomes or elementary events.

Definition. A sample(probability) space of a random experiment is a set S that includes all possible outcomes of the experiment.

Example. If the experiment is to throw a standard die and record the outcome then:
sample space S = {1,2,3,4,5,6} elementary events

Definition. A compound event is a subset of S consisting of several elementary events.

Q. Using the experiment of throwing a die, what is an example of a compound event?

A.
Throwing an even number, E = {2,4,6}
Throwing a prime number, E = {2,3,5}
Throwing a power of 2, E = {1,2,4}

Definition. Let S be the sample space of an experiment and E be an event in S then Laplaces definition of probability says that the probability of E is:

$$Prob(E) = \frac{|E|}{|S|}$$

Q. What is the probability of rolling a 3 on a standard die?

A.
$E = \{3\}, S = \{1, 2, 3, 4, 5, 6\}$
$|E| = 1 \;\; |S| = 6 \;\; Prob(E) = \frac{1}{6}$

Q. What is the probability of rolling a power of two on a standard die?

A.
$E = \{1, 2, 4\}, S = \{1, 2, 3, 4, 5, 6\}$
$|E| = 3 \;\; |S| = 6 \;\; Prob(E) = \frac{3}{6} = \frac{1}{2}$

Bayes Rule.

Theorem (Bayes Rule). Let A and B be events in the same sample space. If neither P(A) nor P(B) are zero, then:

$$\frac{P(B) \cdot P(A|B)}{P(A)}$$

The second is the concept of total probability:

Theorem (Total Probability). Let a sample space S be a disjoint union of events $E+1, E+2, ..., E_n$ with positive probabilities, and let $A \subset S$. Then:

$P(A) = \sum_{i=1}^{n} P(A|E_i) \cdot P(E_i)$

16 Complexity Analysis

When we talk about how good an algorithm is, we often use the terms worst case complexity. This means, the number of steps the algorithm takes for the worst possible input.

Sometimes we care more about the average or expected number of steps.

Example. Searching a list L of integers from left to right. In the following list:

L = 3, 5, 23, 6, 4, 1, 7, 10, 26, 8, 9, 11, 15

if we search by visiting each integer from left to right we will perform 6 visits if we are looking for the number 1 and only 2 visits if we are searching for 5.

Q. How many integers do we visit in the worst case?

A. In general, for a list of length n, n comparisons. (len(L)) Happens when the item we are looking for is on the far right of the list.

Q. If we assume that we are searching for an integer k in the list and that all positions of the list are equally likely to hold the integer we are looking for, what is the probability of finding the integer in the ith position of a list of length n?

Expected Average it's in the list and everything is equally likely.

A. $\frac{1}{n}$

Q. How many steps(comparisons) does it take to find the integer if it is in the ith position?

A. Call this $N(i)$

We compute the expected E(n) number of steps of the algorithm by computing for each of the i positions:

P(k in the i th position) N(i)

and then taking the sum over all n possible values for i

$$\text{E(n)} = \sum_{i=1}^{n} P(\text{k in the ith position}) \cdot N(i)$$

$$= \sum_{i=1}^{n} \frac{1}{n} \cdot i$$

$$= \frac{1}{n} \cdot \frac{n(n+1)}{2} = \frac{n(n+1)}{2}$$