Lecture Notes – COMP2121

Notes by José A. Espiño P.*

Semester 2 2022–2023

Contents

*The contents of this document come from both lectures and the textbook *Discrete Mathematics and its Appplications*, by Kenneth H. Rosen. I do not claim autorship for anything herein.

1 Introduction to Discrete Maths

Discrete Maths are all the mathematical concepts you will need to become a competent computer scientist. It includes topics such as graphs, logic, proofs, sets, relations, counting, probability, and others.

2 Logic

2.1 Propositional Logic

A proposition is a statement that can be **unambiguously** determined to be either true (T) or false (F). T and F are called the truth values of the proposition.
Logic is about making deductions from composite propositions. These are built by using logical operators.

2.1.1 Logical Operators

1. NOT: $\neg p$
   It makes the value of p be the opposite.

2. AND: $p \land q$
   It is only true if both p and q are true.

3. OR: $p \lor q$
   It is true if either p or q are true.

4. EXCLUSIVE OR: $p \oplus q$
   True if either p or q are true, but not both of them.

5. IMPLIES $p \implies q$
   Can be read as "if p, then q," "q if p," "p is sufficient for q," or "q is necessary for p"
   The only case in which it is false is when p is true and q is false.

6. BICONDITIONAL $p \Leftrightarrow q$
   It is true when p and q share the same truth value.

We generally use parentheses to denote the order in which logical operators must be used; however, it is useful to know their precedence: negation is applied before all other operators (which is why it is rarely used alongside brackets). Secondly, the conjunction operator takes precedence over the disjunction operator, so that $p \land q \lor r$ means $(p \land q) \lor r$. Finally, it is an accepted rule that the biconditional and the implication operators have the lowest precedence.

2.1.2 Methods of Propositional Logic

Way to obtain the truth value of composite propositons.
Method number one is using a **Truth Table**. We compute the truth values of a composite proposition case–]by–case from the truth values of its components. We start with the truth value of every variable, then we go with the items in parentheses, and we keep on working from inside to outside until we can span the entire expression. This mehtod is not efficient because the more variables you have, the longer the table becomes.
The second method is to use **Boolean Algebra**. For that, you have to follow a set of algebraic rules:

1. Identify the truth value F with the number 0 and the truth value T with the number 1.

2. Denote by $w(p)$ the truth value of the proposition p.

3. Use the following rules of Boolean Algebra:

   - $w(\neg p) = w(p) \oplus 1$
   - $w(p \land q) = w(p)w(q)$

- $w(p \oplus q) = w(p) \oplus w(q)$
- $w(p \Leftrightarrow q) = w(p) \oplus w(q) \oplus q$
- $w(p \implies q) = w(p)w(q) \oplus w(p) \oplus 1$
- $w(p \vee q) = w(p) \oplus w(q) \oplus w(p)w(q)$

Important: in Boolean Algebra, $\oplus$ is the modulo–2 sum operator. The only numbers that summed together will equal one are zero and one. Every other combination will result in a zero.

Additionally, when you multiply any value by itself, it will result in that value. We do not square it because either one squared or zero squared result in the same value.

The third method is called **Logical Equivalence**. Before introducing this method, it is important to understand the meaning of a **tautology**: a proposition that can only be true. They are commonly denoted as T. An example of a tautology is $p \vee (\neg p)$. Some propositions are logically equivalent, which means that $p \Leftrightarrow q$ is a tautology. When this is the case, we can replace one by the other, and we write $p \equiv q$. It is also important to talka bout the concept of a **contradiction**. This is a proposition that can only be false, and we denote it by F. For example, $p \wedge (\neg p)$. Lastly, a **contingency** is a compound proposition that does not fit into either of the two aforementioned categories. Once we know these concepts, our aim is to reduce a complex proposition to a collection of tautologies or contradictions whose truth value we can easily determine from inspection.

Some of those properties are:

- Double Negation Law: $\neg(\neg p) \equiv p$
- Biconditional Law: $(p \Leftrightarrow q) \equiv (p \implies q) \wedge (q \implies p)$
- Implication Law: $(p \implies q) \equiv (\not p \vee q)$
- Contraposition Law: $(p \implies q) \equiv (\neg q \implies \neg p)$
- De Morgan's Laws: $\neg(p \wedge q) \equiv (\neg p \vee \neg q)$
  $\neg(p \vee q) \equiv (\neg p \wedge \neg q)$
- Distributivity Law: $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$
  $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee \ )$

This is a non–exhaustive list — there are many other useful properties you may need; however, these are the most important that you must memorise by the end of this course.

A common way we employ logical equivalence to solve a complicated proposition is by trying to reduce the amount of logical operators present. The ones that tend to go first are biconditionality and implication.

2.2 Predicate Logic

A **predicate** is a statement $P(x)$ that depends on a variable x, so that $P(x)$ is a proposition for any x possible. There also exist multivariable predicates in the form $P(x, y)$. Predicates are separate from propositions because we cannot unambiguously determine their truth value; this will change based on the value that the variable takes.
For a variable x in a predicate, the set of values that x could possibly assume are called the universe of discourse or the domain.
There are two ways to turn a predicate $P(x)$ into a proposition:

1. Fix x: give a determinate value to the variable.

2. Quantify over x

2.2.1 Quantifiers

- The universal quantifier $\forall$
  it means that $P(x)$ holds for every x in the domain.
  $\forall P(x) \equiv P(a) \land P(b) \land P(c) \land \ldots$

- The existential quantifier $\exists$
  it means that $P(x)$ holds for at least one x in the universe of discourse.
  $\exists x P(x) \equiv P(a) \lor P(b) \lor P(c) \lor \ldots$

Sometimes, the universe of discourse is made explicit in the notation. For example, $\forall n \in N$. Sometimes, we use shorthands notations, such as $\forall x > 0$, which means that the universe of discourse is the set of real numbers.
To guarantee that $\exists x P(x)$ is true, it is enough to find an example x_0 such that $P(x_0)$ is true. Similarly, to guarantee that the proposition $\forall x P(x)$ is false, it is enough to find a counterexample x_0 such that $P(x_0)$ is false.

2.2.2 Logical Equivalences in Predicate Logic

- Negation of $\forall$
  The negation of $\forall x P(x)$ is $\exists x \neg P(x)$

- Negation of $\exists$
  The negation of $\exists x P(x)$ is $\forall x \neg P(x)$

- **Warning!**
  Quantifiers cannot be exchanged arbitrarily.
  $\forall$ cannot be arbitrarily exchanged with $\exists$
  Quantifiers are not always distributive with respect to logical operators.
  $\forall x[P(x) \lor Q(x)]$ is not the same as $[\forall x P(x)] \lor [\forall x Q(x)]$

- What is okay to do?
  Quantifiers of the **same type** can be exchanged.

$\forall$ is distributive with respect to $\wedge$
$\exists$ is distributive with respect to $\vee$

3 Proofs

3.1 Valid Arguments

A **valid argument**is a sequence of logical implications, where, if the premise is true, the conclusion must be true. Recall the logical operation of $p \implies q$:the only case where this preposition is false is when $p = T$ and $q = F$. Logical implication is highly related to this concept: we say that p *logically implies* q if $p \implies q$ is a tautology. In order words, the truth of p can guarantee the truth of q.
With this feature of logical implication, we can create a chain of these.
Intuitively, $p \implies q \equiv T$ when it is harder for p to be true. For example, consider the case of $(p \wedge q \implies q)$.
This is called the **simplification rule**. There is also the case of **Addition**, where we can turn something simple into something more complicated, but thanks to the or operator, we can still satisfy the logical implication. This is in the form: $p \implies (p \vee q)$

3.1.1 Constructing Valid Arguments: the Rules of Inference

Valid arguments are made of logical implications.
In **Propositional Logic**, we have the following tools to construct arguments:

- Modus Ponens:
  $(p \implies q) \wedge p$ logically implies q
- Modus Tolles:
  $(p \implies q) \wedge \neg q$ logically implies $\neg p$
- Hypothetical syllogism
  $(p \implies q) \wedge (q \implies r)$ logically implies $(p \implies r)$
- Disjunctive syllogism
  $p \vee q \wedge \neg p$ logically implies q
- Inference rule
  $(p \vee q) \wedge (\neg p \vee r)$ logically implies $q \vee r$

In **Predicate Logic**, we have the following rules of inference:

- Existential Generalisation
  If you find one $P(x_0) = T$ for some x_0 in the universe of discourse, then we can guarantee that $\exists x P(x)$
- Universal Generalisation
  If you can show that $P(x_0) = T$ for a **generic** x_0 in the domain, we can guarantee that $\forall x P(x)$

- Inference rule
$\forall x P(x)$ logically implies $P(x_0)$ for any fixed x_0 in the universe of discourse.
- Universal modus ponens
$[\forall x(P(x) \implies Q(x))] \wedge P(x_0)$ logically implies $Q(x_0)$
- Existential instantiation
$\exists x P(x)$ logically implies $P(x_0)$ for some x_0 in the universe of discourse.

3.2 Constructing Proofs

A proof is a valid argument that guarantees the truth of a proposition, called the **thesis**. A proof consists of two ingredients: firstly, a set of premises. These are facts that are known to be true; sometimes they are explicit, but they can also be implicit. Secondly, a sequence of logical implications that will eventually reach the thesis.
Direct Proof
You use known facts to prove that q is logically equivalent to p.
Proof by Contraposition
You use known facts to deduce $\neg p$ from $\neg q$. The validity of this argument is based on the contraposition law: $p \implies q \equiv \neg q \implies \neg p$
Proof by Contradiction
The strategy is finding a contradiction F such that $\neg p$ logically implies F. The validity of this argument is also based on the contraposition law: $\neg p \implies F \equiv T \implies p$
Usually when you see "there is no," "does not exist," "for every," it might be useful to try this method.
Proof by Induction
Thesis: you want to show that $P(n)$ is true for a determinate dominion. There are two steps you need to take,

- firstly, you need to prove that $P(1)$ is true.
- Secondly, you assume that $P(k)$ is true, and from that, you must determine that $P(k+1)$ is true.

Proof by Equivalence
Show that $p \implies q$ and that $q \implies p$. This reaches the thesis that $p \equiv q$

4 Sets and Relations

4.1 Sets

Sets are all about classifying objects.
A set is a collection of **distinct objects**. Every object in a set is called an **element**.
Notation:

$x \in A$ means x is an element of A.
$x \notin A$ means x is not an element of set A.
The order of a set does not matter. As long as they share the same elements, two sets will be the same.
There are different ways to define a set:

- Roster Notation:
  Write every element in set explicitly
  If a finite set A contains n elements, $x_1, x_2, \ldots, x_n$, we write it as $A = \{x_1, x_2, \ldots, x_n\}$.

- Set Builder Notation:
  $\{x : x$ has properties P,Q,$\ldots\}$. This reads "the set of all x such that x has properties $P, Q, \ldots$"
  For example, $\{n \in Z : \exists k \in Z, n = 2k + 1\}$ represents all odd numbers.

- Venn Diagrams:
  You put the name of the set on top of a circle that contains all the elements in the set.
  Venn diagrams are not commonly used for definition of sets; however, they serve as a way to discuss about the relationship between different sets. Remark: when reasoning on set relation the elements can be omitted.

Cardinality:
Number of distinct objects in a set, denoted by $\|A\|$
Example: $A = \{x_1, \ldots, x_n\}$, we have $\|A\| = n$
Some sets can have infinite cardinality. In order to compare the cardinality of such sets, we can establish mapping between the elements of each set. For instance, mapping every integer n to a unique member $k = 2n$, where n is the set of real numbers and k is the set of even numbers. We could not do this if we compared n to, for instance, the set of real numbers.
The empty set
Contains no element at all. We use the symbol $\emptyset$. The propositon $x \in \emptyset$ is false by definition, no matter what x is. Also notice that $\|\emptyset\| = 0$
Nested Sets
Sometimes the elements of a set can also be sets. In this case, we count the entire nested set as a single element for cardinality calculation purposes. The empty set also counts like an element, since it is a set in and of itself.
In principle, a set can even **contain itself**! This renders the discussion more complicated, since the set refers to itself recursively. However, for cardinality purposes, we count the set in question as just one element.
This may sometimes lead to paradoxes, such as *Russell's Paradox*:
Let S be the set containing all sets that do not contain themselves. In formula:
$S := \{\text{set } A : A \in A\}$
Since S is a set, this formula leads to contradiction:
If $S \in S$, then by definition of S, SS

If $S \notin S$, then S satisfies the defining property of S, so $S \in S$
Both are contradictions! Undetermined whether S could be a part of this set.
Thus, in this course we will solely deal with well–defined sets. NO self–referencing sets!

4.2 Sets and Predicates

Predicates from Sets Let U be the set of all possible values of the variable x. We can regard U as a universe of discourse for predicate logic.
For every set A, we can define the predicate that depends on A:
$P_A(x) : x \in A$
A predicate statement returns either `true` or `false`.
Viceversa, for every predicate $P(x)$, we can define the truth set using the builder notation:
$A_p = \{x \in U : P(x)\}$, which means the set of all x such that $P(x)$ is true. Here, we would say that $P(x)$ is a **defining feature of its truth set**.
For example, let $U = \{1, 2, 3, 4, 5, 6\}$, $P(x)$: x is odd. Then $A_p = x \in U : x\text{is odd} = 1, 3, 5$

Subsets
Smaller sets included in bigger sets.
A is a subset of B if **every element of A is an element of B**. We write this as $A \subseteq B$. The logical expression for this is $A \subseteq B \equiv \forall x[(x \in A) \implies (x \in B)]$.
Every set is a subset of itself
A is a **Proper subset** of B if $A \subseteq B$ and $A \neq B$. This is written as $A \subset B$
Equality of two sets:
We only use it when both sets contain exactly the same elements.
We use the following logical expression: $A = B \equiv \forall x(A \subseteq B) \wedge (B \subseteq A)$
The Power Set
The Power Set of a given set A is the set containing all subsets of A. The notation we use for it is $P(A)$ or 2^A. Empty set is always a subset of every other set.
Property:
If A is a finite set, then $\|P(A)\| = 2^{\|A\|}$. This is because a subset $S \subseteq A$ is specified by declaring which elements of A are in S and which ones are not. Since there are two possible choices for every elmeent $x \in A$, we obtain the property above.

4.3 Operations with Sets

1. Set Intersection:
   $A \cap B$ is the set of elements that are both in A and B.
   Associated with $\wedge$.
   $x \in A \cap B \equiv (x \in A) \wedge (x \in B)$

2. Set Union:

$A \cup B$ is the set of elements that are in A or B
Associated with $\vee$
$x \in A \cup B \equiv (x \in A) \vee (x \in B)$

3. Set Difference:
   $A - B$ is the set of elements in A but not in B.
   $x \in A - B \equiv (x \in A) \wedge (x \notin B)$

4. Set Complement:
   Elements in U not in A.
   You need to specify what the set U will be!
   Associated with $\neg$
   $x \in \overline{A} \equiv x \notin A$

4.4 Reasoning about Sets

Sets are in one to one correspondence with predicates, thanks to the fact that the properties of logical operations can be used to derive properties of operations with sets.
Some important identities:

- $A \cup \emptyset = A \cap U = A$
- $A \cup B = B \cup A$
- $A \cup U = U$
- $A \cup (B \cup C) = (A \cup B) \cup C$ *This rule also applies for intersection
- $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
- $A \cup A = A \cap A = A$
- $\overline{\overline{A}} = A$
- $\overline{A \cup B} = \overline{A} \cup \overline{B}$
- $\overline{A \cap B} = \overline{A} \cap \overline{B}$

The Cartesian Product of Sets
Denoted as AxB. It's the set containing all elements of the form (x,y) with $x \in A$ and $y \in B$. The elements (x,y) are called **ordered pairs**. The order matters! $(x, y) \neq (y, x)$. When there are more than two sets, the same logic applies, with (x, y) becoming $(x, y, z, \dots)$

4.5 Relations

A relation from A to B is a subset of AxB, which is denoted as $R \subseteq AxB$. We write xRy if $(x, y) \in R$. The order also matters in this case: $xRy \neq yRx$. There are different ways to represent a relation:

- Bipartite Graph:
  Draw the sets A and B, and draw an arrow from x to y if xRy.

- Tables:
  Label the rows by elements of A and the columns by elements of B. The (x, y) entry equals 1 if xRy and 0 otherwise. Tables in this form can also be simplified to a matrix.

- Directed Graph Representation for Relations on a Set:
  A relation on A is a specific type of relation from A to the same set A. It can be represented by all the aforementioned methods, as well as a directed graph. Directed graphs require you to write all the elements in A as **points** and to write an **arrow** from element x to y if xRy.

Special Types of Relations on Sets

- Reflexive Relations
  When every element in the set A is in relation with itself
  $\forall x \in A(xRx)$

- Symmetric Relations
  If in a set A, y is in relation with x whenever x is in relation with y.
  $\forall x, y \in A[(xRy)(yRx)]$

- Transitive Relations
  If xRy and yRz can guarantee xRz
  $\forall x, y, z \in A\{[(xRy) \wedge (yRz) \implies (xRz)]\}$

- Equivalence Relations
  An equivalent relation is a relation R on set A that is at the same time reflexive, symmetric, and transitive. Equivalence classes:
  An equivalent class of x is the set of all elements that are equivalent to x.It is a subset of A. It is most often denoted as $[x]$. Every element of $[x]$ is called a representative of that equivalence class. You can partition A into a different discrete group of classes. If $[x] \cap [y] \neq \emptyset$, then $[x] = [y]$. That is to say, if $A_1 \cap A_2 = \emptyset$, then these two sets are disjoin and are distinct equivalence classes. The distinct equivalence classes form a partition of A. For example, if $A =$ people in Hong Kong and xRy if x and y are born in the same month, A can be partitioned as [Jan], [Feb].[Mar . . .]

5 Functions

5.1 What is a function

A function is essentially assigning elements of one set to those in another set. A more rigurous definiton would be that a function from set A to set B is a special type of relation with the property that every element of A is in relation with **exactly one** element of B. A logical definition would be $(\forall x \in A, \exists y \in B, xRy) \land \forall x \in A, \forall y_1, y_2 \in B, [(xRy_1) \land (xRy_2)] \implies y_1 = y_2$
If a relation R is a function, we write $y = R(x)$ instead of xRy. If R is a function from A to B, we write $A \to B$. Here, A is the **domain** of R and B is the **codomain** of R.
If $y = R(x)$, we say that y is the **image** of x and x is the **preimage** of y.
To define a function. we have to

1. Specify **domain** and **codomain**

2. Specify a rule that assigns every **image** to its **preimage**

This looks like:
$f : A \to B$ $f(x) =$ (rule to compute f(x) from x)
The range of a function $f : A \to B$ is the set of all elements of B that are images of elmeents in A. It is always a subset of codomain B. We denote the range of f as $f(A) = \{y \in B : \exists x \in Ay = f(x)\}$
By definition, the range of f is a subset of the codomain $(f(A) \subseteq B.)$ Sometimes, the range and codomain can be equal.

5.2 Properties of functions

- Injective Functions:
  If for every pairs of x and $x^{'}$ in the domain, $x \neq x^{'}$ implies $f(x) \neg f(x^{'})$
  You show that a function is injective if for every x, x' in A, one has:
  $f(x) = f(x') \implies x = x'$, which is logically equivalent to saying $x \neq x' \implies f(x) \neq f(x')$ because of the contraposition law.
  Basically, if function is one–to–one, it is injective.

- Surjective Functions:
  A function $f : A \to B$ is surjective is for every $b \in B$, there exists some $a \in A$ such that $f(a) = b$
  Basically when the codomain is equal to the range.

- Bijective Functions:
  A function that is both **injective and surjective**.

5.3 Operations on functions

- Composition:
  Given two functions $f : A \to B$ and $g : B \to C$ one can define the

composition $g \circ f : A \to C$ as$g \circ f(x) = g(f(x))$
Apply the rule of the function on the right and plug it into the other one.
For example, let $f : R \to R, f(x) = \sin x$ and $g : R \to R, g(y) = 2^y$, then $g \circ f(x) = 2^{\sin x}$
IMPORTANT: In general if you have a composite function $f \circ g(x)$ for arbitrary functions f, g then in order for the composition to be possible, the range of g must be a subset of the domain of f.

- Inversion:
  Let $f : A \to B$ be a bijective function. Then, there is a function $g : B \to A$ such that $\forall x \in A, g \circ f(x) = x$ and $\forall y \in B, f \circ g(y) = y$. The function g is called the inverse of f and denoted by f^{-1}.
  In short, an inversion of a function f is obtaining the preimage from a given element in the image.

Real–valued functions are those functions in the form $f : A \to B$ if $B \subseteq R$. For the following definitions, let A and B be subsets of R.
A function $f : A \to B$ is called non–decreasing if $\forall x, y \in A, [x \leq y \implies f(x) \leq f(y)]$
A function $f : A \to B$ is called non–increasing if $\forall x, y \in A, [x \geq y \implies f(x) \geq f(y)]$
Strictly increasing and strictly decreasing are defined the same as the two above respectively, but without the equal in the comparison.

5.4 How fast a function can grow

Please consider the word *asymptotic* to mean "for large enough n," where n is the size of the input.

- Big–O notation
  $O(g)$ contains all the functions that grow slower than g. So, for $f \in O(g)$, g is an asymptotic upper bound for f.
  The formal definition of the set $O(g)$ is $O(g) := \{f : N \to R : \exists c > 0, \exists n_0 \in N, \forall n \geq n_0 f(n) \leq cg(n)\}$
  Usually, g is chosen to be a simple function whose speed and growth we know well. This means that we rarely include the coefficients.
  Polynomials:
  $n^a \in O(n^b)$ for $\forall a \geq 0, \forall b \geq a$
  Exponentials:
  $a^n \in O(b^n)$ for $\forall a \geq 1, \forall b \geq a$
  Notice that exponentials grow much faster than polynomials! Thus, programs with exponentially growing running times are considered non–efficient.
  It is common in mathematics to see $f(x) = O(g)$ instead of $f \in O(g)$. In this notation, $=$ is not a true equality, it is just a shorthand way of saying that f is in $O(g)$.

- Big–Ω notation
  $\Omega(g)$ contains all the functions that grow at least as fast as g. Thus, Ω

functionally showcases the lower bound of a function.
Formally, we say that $f(n) = \Omega g(n)$ if there exists $c > 0$ and n_0 such that $\forall n \geq n_0, f(n) \geq cg(n)$
Notice that O and Ω are dual to each other. $f(n) = O(g(n))$ if and only if $g(n) = \Omega(f(n))$. For example, if $n = O(2^n)$ then $2^n = \Omega n$.

- Big–Θ notation:
  $\Theta(g)$ contains all the functions that have g as both their upper and lower bound. We call g an **asymptotic tight bound**. The definition $f(n) = \Theta(g(n))$ is symmetric if and only if $g(n) = \Theta(f(n))$
  When solving exercises that ask you to show that a function $f \in \Theta g$, there are two methods you can follow:
  - Prove that $f(n) = O(g(n))$ and $f(n) = \Omega(g(n))$.
  - prove that there exist two constants c_1, c_2 and an integer n_0 so that the inequality $c_1 g(n) \leq f(n) \leq c_2 g(n)$ holds for any $n \geq n_0$.
- Asymptotic limit for the factorial:
  We can define a lower and upper bound for this function through *Stirling's Bounds*:
  $\sqrt{2\pi}(n^{n+\frac{1}{2}}e^{-n}) \leq n! \leq e(n^{n+\frac{1}{2}}e^{-n})$
  Factorials grow significantly larger than exponentials, because $g(n) = e^{n(ln(n)-1)+\frac{1}{2}ln(n)}$, which is larger than e^n when n is big enough.

6 Counting

Golden Rules of Counting

1. **Product Rule**:
   If a procedure can be broken down into a sequence of two tasks and there are n_1 ways of doing the first task and for each of these two ways of doing the first task, there are n_2 ways of doing the second task, then there are $n_1 n_2$ ways to do the whole procedure.
2. **Sum Rule**:
   IS

6.1 Sets

Let X, Y be two sets with the same cardinality. If there is a bijective function from X to Y, IS wrote the wrong way
Disjoint sets employ the Sum Rule:
Recall that two sets are disjoint if their intersection is empty set. If this is the case for two sets X and Y, then the total amount of elements in both sets equals $\|X \cup Y\| = \|X\| + \|B\|$. ISISISIS

Overlapping Sets: the Inclusion–Exclusion principle:
A way to calculate the cardinality of the union two sets A, B that are not necessarily disjoint. The way we do this is by computing $\|A\| + \|B\| - \|A \cap B\|$
If we have three sets, we can just expand the aforementioned formula as (IS).
Picture for proof: february 20th
There is a general formula for n arbitrary sets that may or not overlap:
copy from pptx
You always start by including, then excluding, then including. It is going to alternate until you get to the last order.
Example: find the amount of integers k with $1 \leq k \leq 100$ that are multiples of 2 or 3 or 5 or 7.
Fact: the number of multiples of x in $\{1, \ldots, n\}$ is FLOOR IS!LL
Cartesian Product: counting couples and triples
Simply employ product rule ISISISISIISISI

6.2 Functions

Write what an indicator function is within example 1.
Example 2
Injectvie:

6.3 Counting Permutations

Banana picture feb 20

6.4 Pigeon

bla bla bla ISL

7 Probability

You assign probabilities by following these steps:

1. Identify a set of alternative outcomes
2. Based on the frequencies of the outcomes, assign a probability to each outcome

In this case, probability quantifies how likely an outcome is to occur. It can be seen as an extension of the truth values of logic, but instead of having the discrete values 0 and 1, it has numbers in the range $0 \leq x \leq 1$.
Formally, probability distributions is defined as follows:
Let S be a **finite** set. The probability distribution over the set S is a real–valued function $p : S \to [0, 1]$. mapping every element $x \in S$ into a probability $p(x)$

and satisfying the condition $\sum_{x \in S} p(x) = 1$. This is because the probability that at least one of the events happen is one. Note that this only applies to finite S!
We might also want to calculate the probability of subsets. Let $p : S \to [0, 1]$ be a probability distribution and $A \subseteq S$ be a subset of S. The probability of the subset A is defined as $P(A) := \sum_{x \in A} p(x)$.
Some basic facts about subsets:

- $P(S) = 1$
- $P(\emptyset) = 0$
- $P(\{x\}) = p(x)$
- $A \subseteq B \implies P(A) \leq P(B)$

In probability theory, the set S is called the sample space (contains all possible outcomes,) the elements of S are called outcomes, and subsets of S are called events.
Assigning Probabilities
There is no rule to picking the probability distribution. Our choice of probability depends on what we know about the mechanism that generates the outcomes. Different people have different pieces of information that may lead to different probabilities. However, on some standard situations there ISL
The uniform distribution is defined as $p(x) = \frac{1}{\|S\|}$, for S being a finite sample space and $\forall x \in S$. In this distribution, $P(A) = \|A\|/\|B\|$. ISL read....
Example: You toss 2 dice. What is the probability that the sum is equal to $n (n \leq 7)$.
Picture provided, february 27.
Example: you pick 5 cards from a deck. What is the probability that none of them form a pair?
inSL

7.1 Composite Events

Let $p : S \to [0, 1]$ be a probability distribution on S and let $A \subseteq S$ and $B \subseteq B$ be two disjoint events ($A \cap B = \emptyset$), then $P(A \cup B) = P(A) + P(B)$.
Let p be a probability distribution on S and let $A \subseteq S$ be an event. Then, $P(\overline{A}) = 1 - P(A)$
Rule of sum of probabilities:

- Disjoint events:
  Let $A_1, A_2, \ldots, A_n$ be mutually disjoin events. Then, $P(A_1 \cup A_2 \cup \ldots \cup A_n)$.
- General case:
  $P(A \cup B) = P(A) + P(B) - P(A \cap B)$

The main take from this is that probability is essentially a generalisation of couting, with each element having a weight.
Union bound ISL!!!!

7.2 Independent Events

7.3 The law of total probability

ISL

7.4 Bayes' Theorem

Example in picture; march 2. Let A and B be two events with $P(A), P(B) > 0$. Then, $P(A|B) = \frac{P(A)P(B|A)}{P(B)}$
Copy Jorge example here.

A Tutorial Problems and their Solutions

This section contains exercises presented in the tutorial lessons of the course MATH2121 on Spring Semester of 2022–2023. They should be treated as reference and support for study, especially considering they have the same formatting as the problems you will meet during the final exam.

A.1 Tutorial 1: Logic

Question 1

- What is the difference between $p \Leftrightarrow q$ and $p \equiv q$?
  The left one is a proposition, whereas $p \equiv q$ means that $p \Leftrightarrow$ is a tautology.
- What is the truth value of $p \implies T$?
  T, since the only way for implication to be false is for the conclusion to be false.
- What does $\forall x, y$ mean?
  It is a shorthand for $\forall x \forall y$

Question 2
Show that the proposition $\neg[\forall x \exists y (P(x) \implies \neg Q(y))]$ is logically equivalent to the proposition $[\exists x P(x)] \wedge [\forall y Q(y)]$

$$\begin{aligned}\neg[\forall x\exists y(P(x) \implies \neg Q(y))] = & \\ &= \exists x\forall y\neg(P(x) \implies \neg Q(y)) \\ &= \exists x\forall y(P(x) \wedge Q(y)) \\ &= \exists x[(\forall y P(x)) \wedge (\forall y Q(y))] \\ &= \exists x[P(x) \wedge (\forall y Q(y))]\end{aligned}$$

Now, the last proposition states that there exists an x_0 such that $P(x_0) \wedge (\forall y Q(y))$ holds. This means that both propositions $P(x_0)$ and $(\forall y Q(y))$ hold, which is logically equivalent to the given proposition.

Question 3

Determine whether $[\neg(\neg p \vee q) \vee (p \wedge r)] \Leftrightarrow (p \wedge q \wedge \neg r)$ is logically equivalent to $\neg p$

$$\begin{aligned}&[\neg(\neg p \vee q) \vee (p \wedge e)] \Leftrightarrow (p \wedge q \wedge \neg r) \\ &\equiv [(p \wedge \neg q) \vee (p \wedge r)] \Leftrightarrow (p \wedge \neg(\neg q \vee r)) \\ &\equiv [p \wedge (\neg q \vee r)] \Leftrightarrow [p \wedge \neg(\neg q \vee r)] \\ &\equiv [p \wedge a] \Leftrightarrow [p \wedge \neg a] && \text{let a }=\neg q \vee r \\ &\equiv (p \wedge a) \oplus \neg(p \wedge \neg a)\end{aligned}$$

Now, use Boolean Algebra

$$\begin{aligned}&\equiv xy \oplus (x(y \oplus 1) \oplus 1) \\ &\equiv xy \oplus xy \oplus x \oplus 1 \\ &\equiv x \oplus 1 \\ &\equiv w(\neg p)\end{aligned}$$

Thus, the statement is proven.

Question 4

Find a counterexample, if possible, to these universally quantified statements, where the universe of discourse for all variables consists of all integers:

- $\forall x\exists y(x = \frac{1}{y})$
  If $x = 0$ then there is no integer for which the statement is true.

- $\forall x\exists y(y^2 - x) < 100$
  If $x = -100$, it is impossible for this to be true. It would require the square of y to be smaller than zero.

- $\forall x\forall y(x^2 \neq y^3)$
  The counterexample is when $x = y = 1$

A.2 Tutorial 2: Proofs

Question 1 — Faulty Proofs
Identify the error(s) in this argument that supposedly shows that:
$if\exists xP(x) \land \exists xQ(x)$ is true, then $\exists x(P(x) \land Q(x))$ is true.

$\exists xP(x) \land \exists xQ(x)$	Premise
$\exists xP(x)$	Simplification from previous step
$P(c)$	Existential instantiation from previous
$\exists xQ(x)$	simplification from first step
$Q(c)$	Existential instantiation from previous step
$P(c) \land Q(c)$	Conjunction from steps three and five
$\exists x(P(x) \land Q(x))$	Existential generalisation

Error: The element c in the existential instantiation steps is different for $P(x)$ and $Q(x)$. We cannot do the conjunction of steps three and five and use the same variable c.

Question 2 — Proof by Induction
Thesis: Every square chessboard of size $2^n x 2^n$ can be covered with $(2x1)$ L–shaped tiles, leaving only one empty square.
In order to solve this question, we need to choose a predicate $P(k)$. In this case, we would say that for a chessboard of size $2^k x 2^k$ and any desired place (x, y) for $(x, y \in \{1, \ldots, 2^k)\}$, there is an L–shaped tile covering the board, leaving only one empty square **at** (x, y).
Secondly, we need to state that for $n = 1$, the board is $2x2$ and $P(1)$ holds.
Next, we need to show that $P(k) \implies P(k + 1)$ for any $k \geq 1$. So, we assume that $P(k)$ holds. We need to show that for a chessboard of size $2^{k+1}x2^{k+1}$ and any desired place (x, y) there is one L–shaped tile covering leaving only one empty square at (x,y).
Here is the key observation: ***A*** $2^{k+1}x2^{k+1}$ ***board is covered by four*** $2^k x 2^k$ ***boards!*** $P(k)$ will clearly apply to each of the four sub–boards.
For any $p = (x, y)$, p must fall within one of the four sub–boards. Let's say the top–left one.
Now, we show that there is a covering leaving only p empty:

1. For the tolp–left sub–board, apply $P(k)$. There exists a covering leaving p empty.

2. For the other sub–boards, apply $P(k)$ with $(2^k + 1, 2^k)$, $(2^k, 2^k + 1)$, and $(2^k + 1, 2^k + 1)$ being empty respectively. We get a covering of each sub–board.

3. Notice that these three empty locations can be covered by an L–shaped tile.

Therefore, combining all four sub–coverings and adding the extra L–shaped tile, we get a covering for the original board with p empty.
Therefore $P(k+1)$ holds! Q.E.D.

Question 3 - Direct and Indirect Proofs
a. Prove that $\max(x, y) + \min(x, y) = x + y$ for all real numbers x and y.
Proof strategy: proof by cases

Case number one: $x \geq y$
$\max(x, y) = x \;\; \min(x, y) = y$
therefore, the result of the sum will be $x + y$
Case number two: $x < y$
$\max(x, y) = y \;\; \min(x, y) = x$
therefore, the result of the sum will be$x + y$

b. Prove that, for every integer n, if n^3 is even, then n is even.
Proof strategy: proof by contrapositions:
Step 1: determine p and q: $p = n^3$ is even
$q = n$ is even
Step 2: negation
$\neg p = n^3$ is odd
$\neg q = n$ is odd
Step 3: prove $\neg q \implies \neg p$
Consider a generic odd number n. We can express it as $2k + 1$ for some integer k.
Then, $n^3 = (2k + 1)^3 = 2(4k^3 + 6k^2 + 3k) + 1$ is odd.
Thus, by the law of contraposition, $p \implies q$

c. Prove that there exist irrational numbers x, y such that x^y is rational.
Proof strategy: direct proof + proof by cases
It is enough to find a pair (x, y) that makes it true.
Step 1 consider the pair $x = y = \sqrt{2}$. There are two cases:

1. $\sqrt{2}^{\sqrt{2}}$ is rational.
   Then, (x, y) is the desired pair. Done!

2. $\sqrt{2}^{\sqrt{2}}$ is irrational.
   Consider a new pair (z, w), where $z = \sqrt{2}^{\sqrt{2}}$ and $w = \sqrt{2}$. Since both are irrational $z^w = {\sqrt{2}^{\sqrt{2}}}^{w=\sqrt{2}} = z = \sqrt{2}^{\sqrt{2}x\sqrt{2}} = 2$, which is a rational number. This gives us the desired pair too!

In summary, there must exist one such pair of (x, y)

A.3 Tutorial 3: Sets and Relations

Question 1
Determine the cardinality of the following sets:

- $A = \{1, p, , \$, \emptyset\}$ The cardinality of this set is 5.
- $B = \{1, \{2, \{3, \{4\}\}\}, 5\}$ The cardinality of this set is 3.
- $C = \hat{A}B$ The cardinality of this set is 1.
- $D = A \cup B$ The cardinality of this set is 7.
- $E = \{x \in Z : x^2 \leq 1\} - \{-1\}$ The cardinality of this set is 2 (zero and one).
- $F = \{(x, y) \in ZxZ : x^2 + y^2 = 13\}$ The cardinality of this set is eight, because $\{(2, 3), (3, 2), (2, -3), (-3, 2), (-2, 3), (3, -2), (-2, -3), (-3, -2)\}$

Question 2
A relation $\succeq$ from a set A to itself is called a *preorder* if it is reflexive and transitive.
A. Let $A = RxR$ and let R be the relation defined by $(x, y)R(x', y')$ if $\|x\| + \|y\| \geq \|x'\| + \|y'\|$. Show that R is a preorder.
Reflexivity: for every $(x, y) \in RxR$, one has $\|x\| + \|y\| \geq \|x\| + \|y\|$. Hence, $(x, y) \succeq (x, y)$
Transitivity: for every $(x_1, y_1), (x_2, y_2)$ and (x_3, y_3) in RxR, one has that $\|x_1\| + \|y_1\| \geq \|x_2\| + \|y_2\|$ and $\|x_2\| + \|y_2\| \geq \|x_3\| + \|y_3\|$ implies $\|x_1\| + \|y_1\| \geq \|x_3\| + \|y_3\|$. Hence, $(x_1, y_1) \succeq (x_2, y_2)$ and $(x_2, y_2) \succeq (x_3, y_3)$ implies $(x_1, y_1) \succeq (x_3, y_3)$
Thus, R is a preorder.

B. Let *succeq* be a preorder on A. Show that the relation $\simeq$ defined by xy if $x \succeq y$ and $y \succeq x$ is an equivalence relation.
Reflexivity: for every $a \in A$, since $\succeq$ is reflexive, one has $a \succeq a$, which implies aa.
Symmetry: For every a and b in A, a means $(a \succeq b) \wedge (b \succeq a)$, which is equivalent to ba.
Transitivity: For every a, b and c in A, ab and bc means $a \succeq b, b \succeq a, b \succeq c, c \succeq b$.
Notice that $\succeq$ is promised to be transitive.
We have $(a \succeq b) \wedge (b \succeq c) \implies (a \succeq c)$ and similarly we can show $c \succeq a$. This means that ac,

C. Let A be a set of propositions generated from a given set of elementary propositions $\{p, q, r, \dots\}$ using the basic logical operations $\{\neg, \wedge, \vee, \oplus, \implies, \Leftrightarrow$

$\}, andlet \rightarrow$ be the relation defined by $p \rightarrow q$ if p logically implies q. Show that $\rightarrow$ is a preorder.
Reflexivity: for every proposition p, the proposition $p \implies p$ is a tautology, because:

$$\begin{aligned} p \implies p &\equiv \neg p \vee p && \text{Implication Law} \\ &\equiv T && \text{Negation law.} \end{aligned}$$

In other words, p logically implies p, and the relation $\rightarrow$ is reflexive.
Transitivity: we have to show that, for all propositions p, q, r the conditions $p \rightarrow q$ and $q \rightarrow r$ imply the condition $p \rightarrow r$. This is equivalent to showing that $(p \implies q) \equiv T$ and $(q \implies r \equiv T)$ imply $(p \implies r) \equiv T$. Note that we have $(p \implies q) \wedge (q \implies r) \rightarrow (p \implies r)$
Substituting the equivalences $(p \implies q) \equiv T$ and $(q \implies r \equiv T)$ into the left–hand–side, we obtain
$T \wedge T \rightarrow (p \implies r)$, which is a tautology.
Now we have the following logical equivalence:

$$\begin{aligned} T \implies (p \implies r) &\equiv \neg T \vee (p \implies r) && \text{implication law} \\ &\equiv F \vee (p \implies r) \\ &\equiv p \implies r \end{aligned}$$

Since $T \implies (p \implies r)$ is a tautology, we obtained that $p \implies r$ is a tautology. This proves that p logically implies r. Hence, $\rightarrow$ is transitive.

Question 3
Let U be a universal set, and let A, B, C be the three subsets of U. Show that:
A.$C \subseteq A \cap B$ if and only if $C \subseteq A$ and $C \subseteq B$
By definition, we have $x \in A \cap B \equiv (x \in A) \wedge (x \in B)$ for any $x \in U$. Therefore, this also holds for any $x \in C$. Since x is a generic element of C, we obtained that $C \subseteq A \cap B$ if and only if $C \subseteq A$ and $C \subseteq B$.

B.$P(A \cap B) = P(A) \cap P(B)$
By definition

$$\begin{aligned} P(A \cap B) &:= \{C \subseteq U : C \subseteq (A \cap B)\} \text{ definition} \\ &= \{C \subseteq U : (C \subseteq A) \wedge (C \subseteq B)\} \text{ part a.} \\ &= \{C \subseteq U : C \subseteq A\} \cap \{C \subseteq U : C \subseteq B\} \text{ definition of intersection} \\ &= P(A) \cap P(B) \text{ definition of power set} \end{aligned}$$

C.$P(A \cup B) \neq P(A) \cup P(B)$, unless $A \subseteq B$ or $B \subseteq A$
Recall that p unless $q = \neg q \implies p$. The statement is logically equivalent to:
$[(A \neg \subseteq B) \wedge (B \neg \subseteq A)] \implies [P(A \cup B) \neq P(A) \cup P(B)]$
Let us prove the above statement:

Recall: to show that $p \implies q$ is a tautology, it is enough to prove $p = T$ logically implies $q = T$.
Assume that the first proposition is true. Since A is not a subset of B, there exists an element $a \in A$ that is not an element of B, namely $a \notin B$. Similarly, since B is not a subset of A, there exists an element $b \in B$ that is not an element of A, namely $b \notin A$.
Hence, $(\{a, b\}\neg \subseteq A) \wedge (\{a, b\}\neg \subseteq B$.
In other words, $(\{a, b\} \notin A) \wedge (\{a, b\} \notin B$.
By definition of union, this means that $\{a, b\}$ is not an element of $P(A) \cup P(B)$.
On the other hand, $\{a, b\}$ is a subset of $A \cup B$, and therefore $\{a, b\} \in P(A \cup B)$
This proves that $P(A \cup B) \neq P(A) \cup P(B)$.

A.4 Tutorial 4: Functions

Question 1 – Big–Θ
Show that $\log n! = \Theta(n \log n)$, where log is the logarithm in base 2.
There are two possible approaches to this question, either proving that $\log n! \in \Omega(n \log n) \wedge \log n! \in O(n \log n)$ or by proving the sandwiched bound of $c_1 f \leq g \leq c_2 f$, where we would need to find constants n_0 and c for the bounds.

The Stirling's Bounds imply

$$\begin{aligned}\log n! \leq & \log e + (n + \frac{1}{2}) \log n - n \log e \\ \leq & \log e + 2n \log n \\ \leq & 2 + 2n \log n\end{aligned}$$

Note that one has $2 \leq n \log n$ for every $n \geq 2$.
Hence, for $n \geq 2$ we have
$\log n! \leq 2n \log n + n \log n = 3n \log n$
Setting $c = 3, n_0 = 2$, this means we have $\log n! \leq cn \log n$ for all $n \geq n_0$ which proves that $\log n! \in O(n \log n)$
Now, we need to work on the other side of the Stirling's Bound to get the BigΩ part.
This is:

$$\begin{aligned}\log n! \geq & \log \sqrt{2\pi} + (n + \frac{1}{2}) \log n - n \log e \\ \geq & n \log n - n \log e\end{aligned}$$

Then,

$$\begin{aligned}loge \leq 2 \leq & \frac{1}{2} n \log n \\ = & \frac{1}{2} n \log n\end{aligned}$$

Setting $c = \frac{1}{2}$ and $_0 = 16$, we have shown that $\log n! \geq cn \log n$ for all $n \geq n_0$.
Hence, $\log n! \in \Omega(n \log n)$
From these two calculations, we can conclude thus that $\log n! \in \Theta(n \log n)$

Question 2 – Function Inversion

Let $f : A \to B$ be an arbitrary function and S be any subset of B. The inverse image of S is the subset of A whose elements are precisely all images of elements of S, denoted by $f^{-1}(S) := \{a \in A : f(a) \in S\}$.

A.

Let $f : R \to R, f(x) = x^2$. Find $f^{-1}(\{1\})$,$f^{-1}([4, 10))$, and $f^{-1}(\{-11\})$.
Note that, unlike the inverse of a function, the inverse image can be defined for any f and does not require f to be bijective.
$f^{-1}(\{1\}) = \{-1, 1\}$
$f^{-1}([4, 10)) = (-\sqrt{10}, -2] \cup [2, \sqrt{10})$
$f^{-1}(\{-11\}) = \emptyset$

B.

Let $f : A \to B$ be an arbitrary function and S, T be subsets of B.
Show that $f^{-1}(S \cup T) = f^{-1}(S) \cup f^{-1}(T)$.
For any $x \in f^{-1}(S \cup T)$, there exists $y \in (S \cup T)$ such that $f(x) = y$. Since $y \in (S \cup T) \equiv (y \in S) \vee (y \in T)$, there are two cases:

- If the case is $y \in S$, then $x \in f^{-1}(S)$ since there is an element of S (namely y) whose preimage is x. This further implies $x \in f^{-1}(S) \cup f^{-1}(T)$
- If the case is $y \in T$, we can prove $x \in f^{-1}(S) \cup f^{-1}(T)$ in the same way as the above case.

Thus, we showed that for any $x \in f^{-1}(S \cup T)$, $x \in f^{-1}(S) \cup f^{-1}(T)$ as well. Therefore, $f^{-1}(S \cup T) \subseteq f^{-1}(S) \cup f^{-1}T$
Next, consider any $x \in f^{-1}(S) \cup f^{-1}(T)$. Since $x \in f^{-1}(S) \cup f^{-1}(T) \equiv (x \in f^{-1}(S)) \vee (x^{-1}(T))$, we have two cases: beginitemize

If $x \in f^{-1}(S)$, then by definition $\exists y \in S : f(x) = y$. Since $y \in S \implies y \in (S \cup T)$ and $f(x) = y$, we have $x \in f^{-1}(S \cup T)$.

If $x \in f^{-1}(T)$, we can prove $x \in f^{-1}(S \cup T)$ the same way
In summarey, we showed that for any $x \in f^{-1}(S) \cup f^{-1}(T)$, $x \in f^{-1}(S \cup T)$ as well. Therefore, $f^{-1}(S) \cup f^{-1}(T) \subseteq f^{-1}(S \cup T)$.
We have proven both $f^{-1}(S) \cup f^{-1}(T) \subseteq f^{-1}(S \cup T)$ and $f^{-1}(S \cup T) \subseteq f^{-1}(S) \cup f^{-1}T$. Therefore, the two sets are equal.

C.

Let $f : A \to B$ be an arbitrary function and S be a subset of B.
Show that $f^{-1}(\overline{S}) = \overline{f^{-1}(S)}$
First, consider $x \in f^{-1}(\overline{S})$. This means that there exists a unique y such that $(y \in \overline{S}) \wedge (y = f(x))$, since for any $x \in A$, its image is unique.

This implies that, for any $y \in B$, $y = f(x) \implies y \notin S$. Consequently, $x \notin f^{-1}(S)$.
We have shown $x \in f^{-1}(\overline{S}) \implies x \in \overline{f(S)}$. This, as well as proving $(x \in f^{-1}(S) \implies x \in f^{-1}(\overline{S}))$ for any $x \in A$ complete the proof.

Question 3 – Recursion and Big–Ω
Let $f : N \to R^+$ be a function satisfying $f(1) = 1$ and $f(n) \leq 2f(n-1) + n$ for every $n \geq 2$. Find an asymptotic upper bound for f.
To solve a recursion problem like the one presented here, you can follow the instruction given for a few steps to find a pattern.

For a generic $n \geq 2$ we have

$$\begin{aligned} f(n) &\leq 2^k f(n-k) + \sum_{j=0}^{k-1}(n-j)2^j \\ &\dots \\ &= 2^{n-1}f(1) + \sum_{k=0}^{n-2}(n-k)2^k \\ &= \sum_{k=0}^{n-1}(n-k)2^k \\ &= n(\sum_{k=0}^{n-1} 2^k) - (\sum_{k=0}^{n-1} k2^k) \end{aligned}$$

The two summations can be done using known equations for the *geometric sum.* For every $l \in N$ and every $x \in R$ such that $n \neq 1$, one has that $\sum_{k=0}^{l} x^k = \frac{x^{l+1}-1}{x-1}$. Using this equation for $x = 2, l = n-1$, we obtain $\sum_{k=0}^{n-1} 2^k = 2^n - 1$.
The second summation in equation one $(\sum_{k=0}^{n-1} k2^k)$ can be done by taking the derivative with respect to x on both sides of the equation for the geometric sum. This eventually gives us $\sum_{k=0}^{n-1} k2^k = n2^n - 2^{n+1} + 2$.
Substituting these two into the first equation we have, we obtain:
$f(n) \leq n2^n - n - n2^n + 2^{n+1} - 2 = 2^{n+1} = 2.2^n$
Thus, $f(n) \in O(2^n)$.

A.5 Tutorial 5: Counting

Binomial Coefficients have the following properties:

- Symmetry: $\binom{n}{m} = \binom{n}{n-m}$ for any $m \leq n$
- Sum: $\sum_{m=0}^{n} \binom{n}{m} = 2^n$
  A general formula for this is $(x+y)^n = \sum_{m=0}^{n} \binom{n}{m} x^m y^{n-m}$
  This can be seen physically through *Pascal's Triange.*

- Recursive Formula: $\binom{n}{m} = \binom{n-1}{m-1} + \binom{n-1}{m}$ for $n > m \geq 1$. Proof in picturen feb 23.
- Chu–Vandermonde: $\binom{n}{m} = \sum_{k=0}^{\min\{m,r,n-r\}} \binom{r}{k}\binom{n-r}{m-k}$ for any natural number $r \leq n$. The previous property is a special case of this one, where $r = 1$. A visual proof of this identity will be provided in a picture; february 23. The one in the picture is when we choose $r = 2$

Question 1 – Combinations and Permutations
Determine how many:
A.
Bit strings contain m zeroes and n ones, and have the property that no pair of zeros are adjacent to each other.
Picture is provided, but $\binom{n+1}{m}$
B.
Ways a student can arrange m distinct math books and n distinct novels on a shelf, with the property that no two math books are adjacent to one another.
Question 2 – Pigeonhole Principle
For 30 days, a student solves at least one exercise of discrete mathematics, Knowing that the total number of exercises solved by the student is no more than 50, show that there exist integers i and j, with $i > j$, such that the student has solved exactly 7 exercises between the end of day j and the end of day i.

A.6 Tutorial 6: Probability

Question 1

B Math Commands for LaTeX

B.1 Logic

Commands that are useful in outputting logicrelated computations.

Term	Symbol	LaTeX
There exists at least one	$\exists$	`\exists`
There exists one and only one	$\exists!$	`\exists!`
Oplus	$\oplus$	`\oplus`
For all	$\forall$	`\forall`
Not	$\neg$	`\neg`
Or	$\lor$	`\lor`
And	$\land$	`\land`
Division	$\div$	`\div`
Implies	$\implies$	`\implies`
if and only if, iff	$\iff$	`\iff`
equivalence	$\Leftrightarrow$	`\Leftrightarrow`
Right implication	$\Rightarrow$	`\Rightarrow`
Left implication	$\Leftarrow$	`\Leftarrow`
Logical Equivalence	$\equiv$	`\equiv`

B.2 Set Theory

Commands that are useful for discussing about sets.

Term	Symbol	LaTeX
Empty Set	$\emptyset$	`\emptyset`
Set of Natural Numbers	N	`\mathbb{N}`
Set of Integers	Z	`\mathbb{Z}`
Set of Rational Numbers	Q	`\mathbb{Q}`
Set of Algebraic Numbers	A	`\mathbb{A}`
Set of Real Numbers	R	`\mathbb{R}`
Is member of	$\in$	`\in`
Is not member of	$\notin$	`\notin`
Owns (has member)	$\ni$	`\ni`
Is proper subset of	$\subset$	`\subset`
Is subset of	$\subseteq$	`\subseteq`
Is proper superset of	$\supset$	`\supset`
Is superset of	$\supseteq$	`\supseteq`
Set union	$\cup$	`\cup`
Set intersection	$\cap$	`\cap`
Infinity	∞	`\infty`

B.3 Functions

Commands that are useful for presenting functions and describe their asymptotic growth.

Term	Symbol	LaTeX
Composition Operator	$\circ$	`\circ{}`
Big Oh	O	O
Big Omega	Ω	`\Omega{}`
Big Theta	Θ	`\Theta`
Floor Division Left	$\lfloor$	`\lfloor{}`
Floor Division Right	$\rfloor$	`\rfloor{}`
Ceiling Division Left	$\lceil$	`\lceil{}`
Ceiling Division Right	$\rceil$	`\rceil{}`

B.4 Counting