Discrete Mathematics
Lecture Notes

Yehuda Lindell
Department of Computer Science
Bar-Ilan University, Israel

November 15, 2015

Abstract

These are lecture notes for a first year undergraduate course in Discrete Mathematics in the Computer Science Department at Bar-Ilan University. These notes contain the technical material covered but do not include much of the motivation and discussion that is given in the lectures. It is therefore not intended for self study, and is not a replacement for what we cover in class.

Contents

Course Aims and Syllabus

Course aims:

1. Develop mathematical language needed for entire degree
2. Learn how to prove: needed for many courses throughout the degree; understand the role that proofs play in mathematics and theoretical computer science
3. Learn how to think in an exact and precise manner: needed for the degree and anything you will do in the field

Course Topics:

1. Basic logic
2. Quantifiers and predicate logic
3. Proof methods
4. Mathematical induction
5. Basic set theory
6. Relations
7. Functions
8. Infinite sets and cardinality
9. Basic combinatorics
10. Recursion
11. Graph theory

Administrative issues: The course requirements, as described in the syllabus, are the exam and a midterm test, passing at least 80% of the exercises, and passing at least 80% of the weekly tests in the moodle system.

1 Basic Logic

1.1 Background

Examples – propositions or statements:

1. "Today is Thursday" is a proposition
2. "There are infinitely many numbers" is a proposition
3. "What is the time?" is not a proposition
4. "Don't drive fast" is not a proposition

Any proposition is either true (T) or false (F) (for this reason, "what is the time?" is not a proposition). We sometimes may not know whether or not a proposition is true or false, but this must be the case.

1. The proposition "there are infinitely many prime numbers" is true, but how do we know this?
2. The proposition "every set of numbers has a minimum" is false, but how do we know this?
3. We do not know whether or not the proposition "there are infinitely many twin primes (i.e., primes p such that p and $p+2$ are both prime)" is true or false.

Deductive reasoning: Deductive reasoning can be carried out on propositions only.

1. The following is an example of valid deductive reasoning (go through the analysis):
   - It will either rain or snow tomorrow.
   - It's too warm for snow.
   - Therefore, it will rain tomorrow.
2. The following is an example of invalid deductive reasoning:
   - If I am sick tomorrow, I will not go to work.
   - I will not be sick tomorrow.
   - Therefore, I will go to work tomorrow.

The analysis of propositions is independent their content. Denote by p the proposition "It will rain tomorrow", by q the proposition "it will snow tomorrow". Then, the first series of propositions is:

- p or q
- Not q
- Therefore p

As such, it can be analyzed logically. If correct, then the conclusion should hold whenever the premises hold.

1.2 Logical Connectives and Truth Tables

The proposition p above is a simple or atomic proposition since it makes a single statement; in contrast, the proposition "p or q" is a compound proposition. We will look at operations for combining propositions; these are called logical connectives. The truth of a compound proposition will depend only on the truth of its component simple propositions, and on the connectives used. We will use truth tables to determine the truth of a compound proposition.

Negation ($\neg$): For any proposition p we denote by $\neg p$ its negation. The truth table is as follows:

p	$\neg p$
T	F
F	T

It is common to also denote negation by $\overline{p}$, p' and $\tilde{p}$.

Conjunction – AND ($\wedge$): This connective is used to say that the compound proposition is true if both components are true.

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

It is also common to denote this connective by $p\&q$ or $p \cdot q$.

Disjunction – OR ($\vee$): This connective is used to say that the compound proposition is true if at least one of the components is true. This is called an inclusive OR since it is true also when both simple propositions are true.

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

It is also common to denote this connective by $p + q$.

Exclusive OR ($\oplus$): This connective is used to say that the compound proposition is true if exactly one of the components is true. This is called an exclusive OR since it is not true when both simple propositions are true, in contrast to the inclusive OR above. This is also a disjunction.

p	q	$p \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

It is also common to denote this connective by $p \veebar q$. An exclusive OR makes sense in a proposition like "Tomorrow I will either go to work or I will go to the beach". The intention of such a sentence is clearly that I will do only of the two, but not both.

Compound propositions – combining connectives: Truth tables are very effective for analyzing compound propositions. Analyze the following sentence:

It is not true that (Paris is not the capital of France and the pope does not live in Rome)

Denote: p =Paris is the capital of France; q =The Pope lives in Rome. Then, the compound proposition is $\neg(\neg p \wedge \neg q)$. In order to analyze this proposition, we will construct a truth table:

p	q	$\neg p$	$\neg q$	$\neg p \wedge \neg q$	$\neg(\neg p \wedge \neg q)$
T	T	F	F	F	T
T	F	F	T	F	T
F	T	T	F	F	T
F	F	T	T	T	F

Once we have this truth table, we can determine the truth of the proposition by plugging in the truth values of p and q and obtaining the result. The logical analysis thus becomes "mechanical".

Observe that the original proposition is equivalent to "Paris is the capital of France or the Pope lives in Rome" (look at the last column of the truth table). As we will see, it is possible to prove that the proposition $\neg(\neg p \wedge \neg q)$ *is always equivalent* to $p \vee q$ which is what we have seen.

It is important to note that the *mathematical* and *logical* use of connectives is not always the same as used in common language. For example, consider the politician's proposition: "It is not true that the peace process is useless". Logically, we analyze this by denoting $p =$ the peace process is useful. Then, the proposition is $\neg(\neg p)$ which equals p (this can be easily seen by using the truth table method: double negation returns to the original proposition). Thus, logically this is equivalent to saying that the peace process is useful. However, clearly this is not what the politician meant (rather s/he means to say that s/he took no position). Nevertheless, we do not accept such ambiguity in science, and certainly not in mathematics.

Question: how many rows are in a truth table with n simple (atomic) propositions?

Conditional proposition – implication ($\Rightarrow$): This connective is used to say that if one proposition is true then so is the other. The first proposition is called the premise and the second proposition is called the conclusion. The basis for filling out the truth table here is that "if p then q" can only be false if p is true and q is false. This is because "if p then q" exactly means that "if p is true then q is also true". However, it means nothing when p is false. Consider the following proposition: "if I pass my exams then I will have a party". The student making this proposition is saying nothing about what she will do if she does not pass her exams. Thus, if the student fails she may or may not have a party, and this does not contradict the proposition. In general, an implication of the form $p \Rightarrow q$ is only a claim about q when p is true; when p is false, nothing is claimed about q and thus the proposition is always correct. We therefore have the following truth table:

p	q	$p \Rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

As a result of the fact that whenever a premise is false then the conclusion is always true, propositions like "if pigs can fly then I am the smartest person in the world" are always true.

If $p \Rightarrow q$ then p is a sufficient condition for q, and q is a necessary condition for p. An implication is often denoted $p \rightarrow q$.

Biconditional proposition ($\Leftrightarrow$): This connective is used to show equivalence between two simple propositions; either both are true or both are false. Formally, we can define $p \Leftrightarrow q$ if $(p \Rightarrow q) \wedge (q \Rightarrow p)$. In mathematical terminology, a biconditional proposition is expressed by saying *if and only if* (or *iff*).

p	q	$p \Leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Operator precedence: when given a compound proposition without parentheses, the order of precedence is: negation, conjunction, disjunction, implication, biconditional implication. This can be very confusing since $p \Rightarrow q \wedge q \Rightarrow p$ is actually $p \Rightarrow (q \wedge q) \Rightarrow p$. Thus, it is recommended to include all parentheses, with the exception of negation before a simple proposition.

1.3 Tautologies and Contradictions

Definition 1.1 *A* tautology *is a compound proposition which is true for all truth assignments of its simple propositions. A* contradiction *is a compound proposition which is false for all truth assignments of its simple propositions.*

Examples:

1. $p \vee \neg p$ is a tautology (it will either rain tomorrow or it won't)
2. $p \wedge \neg p$ is a contradiction
3. $(p \wedge q) \vee \neg(p \wedge q)$ is a tautology (simply by appealing to (1))

Tautologies and contradictions are in some sense uninteresting propositions. For example, telling someone that it will either rain tomorrow or will not provides no information whatsoever.

1.4 Logical Equivalence and Implication

Definition 1.2 *Two proposition A and B are* equivalent*, denoted $A \equiv B$, if they define the same truth table on their atomic propositions. All tautologies are equivalent, and all contradictions are equivalent.*

We remark that $A \Leftrightarrow B$ and $A \equiv B$ are not the same; the former is a new compound proposition, whereas the latter is a mathematical claim about A and B. The connection between them is that the compound proposition $A \Leftrightarrow B$ is a *tautology* if and only if $A \equiv B$.

Example 1.3 *We claim that $p \Leftrightarrow q$ is equivalent to $\neg(p \veebar q)$. The most straightforward way to prove such a proposition is to write out the truth table:*

p	q	$p \Leftrightarrow q$	$p \veebar q$	$\neg(p \veebar q)$
T	T	T	F	T
T	F	F	T	F
F	T	F	T	F
F	F	T	F	T

Example 1.4 *Our aim is to find a simple equivalent proposition to $\neg p \Rightarrow (q \vee (r \wedge \neg p))$. This is complicated, so we first construct a truth table:*

p	q	r	$\neg p$	$r \wedge \neg p$	$q \vee (r \wedge \neg p)$	$\neg p \Rightarrow (q \vee (r \wedge \neg p))$
T	T	T	F	F	T	T
T	T	F	F	F	T	T
T	F	T	F	F	F	T
T	F	F	F	F	F	T
F	T	T	T	T	T	T
F	T	F	T	F	T	T
F	F	T	T	T	T	T
F	F	F	T	F	F	F

It is now easy to see that this proposition is equivalent to $p \vee q \vee r$, which is much easier to understand. Nevertheless, saying "you must do all exercises or pass the midterm test or pass the exam" is exactly the same as saying "if you don't do all the exercises then either you must pass the midterm test or (you must pass the exam and not do all exercises)".

Definition 1.5 *Proposition A* logically implies *proposition B, denoted $A \vdash B$ or $A \therefore B$, if whenever A is true then B is true.*

Similarly to equivalence and tautologies, we have that $A \vdash B$ if and only if $A \Rightarrow B$ is a tautology.

Example 1.6 *Show that q logically implies $p \vee q$. This is shown easily via the truth table:*

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

It follows that whenever p is true, then $p \vee q$ is also true. Consider another truth table, including the proposition $(q \Rightarrow (p \vee q))$:

p	q	$p \vee q$	$q \Rightarrow (p \vee q)$
T	T	T	T
T	F	T	T
F	T	T	T
F	F	F	T

Thus, $(q \Rightarrow (p \vee q))$ is a tautology, as required.

Example 1.7 *Show that $p \Rightarrow q$ is equivalent to $\neg q \Rightarrow \neg p$. We construct the truth table:*

p	q	$p \Rightarrow q$	$\neg q \Rightarrow \neg p$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

This equivalence is of particular importance since it tells us that instead of proving $p \Rightarrow q$ we can prove $\neg q \Rightarrow \neg p$. This proof technique is often used and is called proving using the contrapositive.

1.5 Equivalence Laws

There are a number of important equivalence laws. We begin with *replacement laws*:

Idempotent laws:

$$\begin{aligned} p \wedge p &\equiv p \\ p \vee p &\equiv p \end{aligned}$$

Absorption laws:

$$\begin{aligned} p \vee (p \wedge q) &\equiv p \\ p \wedge (p \vee q) &\equiv p \end{aligned}$$

Commutative laws:

$$\begin{aligned} p \wedge q &\equiv q \wedge p \\ p \vee q &\equiv q \vee p \\ p \veebar q &\equiv q \veebar p \\ p \Leftrightarrow q &\equiv q \Leftrightarrow p \end{aligned}$$

Associative laws:

$$\begin{aligned} (p \wedge q) \wedge r &\equiv p \wedge (q \wedge r) \\ (p \vee q) \vee r &\equiv p \vee (q \vee r) \\ (p \veebar q) \veebar r &\equiv p \veebar (q \veebar r) \\ (p \Leftrightarrow q) \Leftrightarrow r &\equiv p \Leftrightarrow (q \Leftrightarrow r) \end{aligned}$$

Distributive laws:

$$\begin{aligned} p \wedge (q \vee r) &\equiv (p \wedge q) \vee (p \wedge r) \\ p \vee (q \wedge r) &\equiv (p \vee q) \wedge (p \vee r) \end{aligned}$$

Involution law:

$$\neg(\neg p) \equiv p$$

De Morgan's laws:

$$\begin{aligned} \neg(p \vee q) &\equiv \neg p \wedge \neg q \\ \neg(p \wedge q) &\equiv \neg p \vee \neg q \end{aligned}$$

Identity laws: Denote by f a contradiction and by t a tautology.

$$\begin{aligned} p \vee f &\equiv p \\ p \wedge t &\equiv p \\ p \vee t &\equiv t \\ p \wedge f &\equiv f \end{aligned}$$

Complement laws:

$$\begin{aligned} p \vee \neg p &\equiv t \\ p \wedge \neg p &\equiv f \\ \neg f &\equiv t \\ \neg t &\equiv f \end{aligned}$$

Transposition law:

$$p \Rightarrow q \equiv \neg q \Rightarrow \neg p$$

Material implication law:

$$p \Rightarrow q \quad \equiv \quad \neg p \vee q$$

Material equivalence laws:

$$\begin{aligned} p \Leftrightarrow q &\equiv (p \Rightarrow q) \wedge (q \Rightarrow p) \\ p \Leftrightarrow q &\equiv (p \wedge q) \vee (\neg p \wedge \neg q) \end{aligned}$$

Exportation law:

$$(p \wedge q) \Rightarrow r \quad \equiv \quad p \Rightarrow (q \Rightarrow r)$$

We remark that the *associative* laws are important since they mean that parentheses are of no importance in a series of ANDs or in a series of ORs. That is, $p \wedge (q \wedge (r \wedge s) \wedge t) = p \wedge q \wedge r \wedge s \wedge t$.

The substitution rule: Let A and B be two propositions such that $A \equiv B$. Let C be a proposition that contains A, and let D be the proposition obtained by replaced A with B in C. Then, the substitution rule states that $C \equiv D$.

Example 1.8 *Our aim is to prove that* $(\neg p \wedge q) \vee \neg(p \vee q) \equiv \neg p$. *Instead of using the truth table method, we now use the above equivalence rules:*

$$\begin{aligned} (\neg p \wedge q) \vee \neg(p \vee q) &\equiv (\neg p \wedge q) \vee (\neg p \wedge \neg q) && \text{(De Morgan)} \\ &\equiv \neg p \wedge (q \vee \neg q) && \text{(Distributive)} \\ &\equiv \neg p \wedge t && \text{(Complement)} \\ &\equiv \neg p && \text{(Identity)} \end{aligned}$$

1.6 Arguments and Formal Proofs of Validition

Definition 1.9 *An* argument *is a set of propositions, called* premises*, together with another proposition called the* conclusion*. An argument is* valid *if the conjunction of the premises logically implies the conclusion; otherwise it is* invalid*.*

Based on what we have seen, an argument is of the form $(P_1 \wedge P_2 \wedge \cdots \wedge P_n) \vdash Q$ and it is valid if and only if the proposition $(P_1 \wedge P_2 \wedge \cdots \wedge P_n) \Rightarrow Q$ is a tautology. (We use capital P_i and Q here in order to stress that each of the premises and conclusion can itself be a compound proposition, and not just a simple one.)

Formal proofs: In order to verify the validity of an argument, one can construct a truth table. However, this is a tedious and long process, especially if the number of premises is large. An alternative method is therefore to construct a sequence of propositions, starting from the premises and leading to the conclusion. In more detail, we begin with the premises and add propositions; a proposition can be added to the list of premises as long as it is *logically implied* by the premises derived so far. The proof of validity is complete when the conclusion is guaranteed by the premises (or, equivalently, if it can be added to the list of premises).

As we have mentioned, in order to add a proposition to the list of premises, it must be logically implied. There are common *rules of inference*, which are very useful in constructing formal proofs. We list these now:

Name of rule	Premises	Conclusion
Simplification	$P \wedge Q$	P
Addition	P	$P \vee Q$
Conjunction	P, Q	$P \wedge Q$
Disjunctive syllogism	$P \vee Q$, $\neg P$	Q
Modus ponens	P, $P \Rightarrow Q$	Q
Modus tollens	$P \Rightarrow Q$, $\neg Q$	$\neg P$
Hypothetical syllogism	$P \Rightarrow Q$, $Q \Rightarrow R$	$P \Rightarrow R$
Absorption	$P \Rightarrow Q$	$P \Rightarrow (P \wedge Q)$
Constructive dilemma	$P \Rightarrow Q$, $R \Rightarrow S$, $P \vee R$	$Q \vee S$

We give two examples of formal proofs using the above rules of inference:

Example 1.10 *We construct a proof that $(p \Rightarrow q) \wedge (p \wedge r) \vdash q$. The premises are $p \Rightarrow q$, $p \wedge r$, and the conclusion is q.*

1. *Premises: $p \Rightarrow q$, $p \wedge r$; using simplification we add p*
2. *Premises: $p \Rightarrow q$, $p \wedge r$, p; using Modus ponens we add q*
3. *q is the conclusion, and thus this completes the proof.*

Example 1.11 *We construct a proof that the premises $(p \Rightarrow q), (r \Rightarrow s), \neg q, r$ imply the conclusion $\neg p \wedge s$. Before we begin, we work out a strategy. Since we wish to prove $\neg p \wedge s$, it will suffice to add both $\neg p$ and s to our list of premises and then apply the conjunction rule.*

1. *Premises: $(p \Rightarrow q), (r \Rightarrow s), \neg q, r$; applying modus tollens to $p \Rightarrow q$ and $\neg q$ we can add $\neg p$*
2. *Premises: $(p \Rightarrow q), (r \Rightarrow s), \neg q, r, \neg p$; applying modus ponens to r and $r \Rightarrow s$ we can add s*
3. *Premises: $(p \Rightarrow q), (r \Rightarrow s), \neg q, r, \neg p, s$; applying conjunction to $\neg p$ and s, we can add $\neg p \wedge s$*
4. *This completes the proof.*

1.7 Quantifiers and Predicate Logic

Assume that we wish to write a proposition expressing the fact that both Alice and Bob are computer science students. We could denote by p that Alice is a computer science student, and by q that Bob is a computer science student, and then write $p \wedge q$. However, this misses the main point that both Alice and Bob study the same subject. A predicate describes a property of objects. We can therefore define the predicate $CS(x)$ to mean that the object x studies computer science. Then, denote Alice by x and Bob by y, we can express our proposition by writing $CS(x) \wedge CS(y)$. The letters x and y are variables, and the predicate CS is called a propositional function. As with simple statements, we can negate predicates $\neg CS(x)$ means that x is *not* a computer science student.

Sets and quantifiers: We often wish to express statements like "all computer science students work hard" or "some computer science students work hard". In order to express this type of statements we first need to to be able to express the concept of the set of all computer science students. A set is a collection of objects, each object in the collection is called an element of the set. For example, let $A = \{1, 2, 5, 7\}$. Then, 2 is an element of A, and 3 is not an element of A. We denote this by $2 \in A$ and $3 \notin A$. We can now define A to be the set of all computer science students. However, this is still not enough to make statements about all or some of these students (or, elements in the set). In order to do this, we need quantifiers.

- **The universal quantifier:** The universal quantifier is used to refer to *all* elements in a set, and is denoted $\forall$. Thus, we can refer to all computer science students by writing $\forall x \in A$. Now, let W be a predicate such that $W(x)$ is true if x works hard. Then, the proposition "all computer science students work hard" can be expressed by $\forall x \in A : W(x)$.

- **The existential quantifier:** The existential quantifier is used to refer to *some* elements in a set, and is denoted $\exists$. Thus, we can refer to some computer science students by writing $\exists x \in A$. Using this notation, the proposition "some computer science students work hard" can be expressed by $\exists x \in A : W(x)$.

  The statement $\exists x \in A : W(x)$ is true as long as there is at least one computer science student that works hard. However, we often wish to say that there exists *exactly one* member of the set for which the predicate holds. We denote this by $\exists!$. Thus, $\exists! x \in A : W(x)$ means that there is exactly one computer science student that works hard; if there are two or more then the proposition will be false.

We remark that it is possible to write propositional functions with more than one variable. For example, $P(x, y)$ can express the fact that $y > x$. Denoting the set of natural numbers by $\mathbb{N}$, we can make statements like $\forall x \in \mathbb{N} \exists y \in \mathbb{N} : P(x, y)$, which means that every natural number has a number larger than it.

We stress that the order of the quantifiers is crucial. For example, if we were to write $\exists x \in \mathbb{N} \forall y \in \mathbb{N} : P(x, y)$ then this would mean that there exists a natural number that is smaller than all the natural numbers. This is a very different statement (note that it is incorrect since there is no requirement that $x \neq y$ and thus the smallest number must also be smaller than itself). Note also that the statement $\exists y \in \mathbb{N} \forall x \in \mathbb{N} : P(x, y)$ is false since this states that the set of natural numbers has a number larger than all natural numbers. Finally, we remark that when the same quantifier is repeated then the order is inconsequential. Thus $\forall x \in \mathbb{N} \forall y \in \mathbb{N} : P(x, y)$ is equivalent to $\forall y \in \mathbb{N} \forall x \in \mathbb{N} : P(x, y)$ and likewise with the existential quantifier.

Negation of quantified propositions: What is the negation of "there exists a computer science student who works hard"? The answer is: "no computer science students work hard", or equivalently "every computer science student doesn't work hard". Likewise, the negation of "every computer science student works hard" is "there exists a computer science student that doesn't work hard". Thus, we have the following negation rules:

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

What about multiple variables? The same rules hold. Specifically, the negation of "every natural numbers has a number larger than it" is "there exists a natural number which has no number larger than it" (i.e., the set has a maximum). Likewise, the negation of "there exists a natural number that is smaller than all natural numbers"? The answer is "every natural number has a number larger than it". That is,

- The negation of $\forall x \exists y : P(x, y)$ is $\exists x \forall y : \neg P(x, y)$
- The negation of $\exists x \forall y : P(x, y)$ is $\forall x \exists y : \neg P(x, y)$

This is actually derived from the basic negation rules as follows:

$$\neg(\forall x \exists y : P(x, y)) \equiv \neg \forall x (\exists y : P(x, y)) \equiv \exists x \neg (\exists y : P(x, y)) \equiv \exists x \forall y : \neg P(x, y)$$

Arguments in predicate logic: The rules of inference that we saw above are all valid in the case of predicate logic as well. However, we need to extend them to deal with quantified propositions. There are four rules of relevance here; we let A denote the set of all elements under discussion:

- **Universal specification:** If $\forall x F(x)$ is true, then $F(a)$ is true for every $a \in A$
- **Universal generalization:** If $F(a)$ is true for every $a \in A$, then the proposition $\forall x F(x)$ is true
- **Existential specification:** If $\exists x F(x)$ is true, then $F(a)$ is true for some $a \in A$
- **Existential generalization:** If $F(a)$ is true for some $a \in A$, then the proposition $\exists x F(x)$ is true

These rules may seem trivial, but are actually the way most mathematical theorems are proven. For example, we often begin by saying "let $\epsilon > 0$", and we then work with this specific ϵ. This is an example of universal specification.

Example 1.12 *We show that the following argument is valid: "All students go to parties and some students drink too much. Therefore, some people who drink too much go to parties." Let A be the set of all people. We define the following predicates:*

- *$S(x)$: x is a student*
- *$D(x)$: x drinks too much*
- *$P(x)$: x goes to parties*

We now construct the proof. The premises are $\forall x(S(x) \Rightarrow P(x))$ and $\exists x(S(x) \wedge D(x))$; the conclusion is $\exists x(D(x) \wedge P(x))$.

1. *Premises: $\forall x(S(x) \Rightarrow P(x))$, $\exists x(S(x) \wedge D(x))$*
2. *Using existential specification, we add $S(a) \wedge D(a)$* [This is like saying: let a be a student that drinks too much]
3. *Using universal specification, we add $S(a) \Rightarrow P(a)$*
4. *Using simplification, we add $S(a)$*
5. *Using modus ponens, we add $P(a)$*
6. *Using the commutative law and simplification to $S(a) \wedge D(a)$, we add $D(a)$*
7. *Using conjunction, we add $D(a) \wedge P(a)$*
8. *Using existential generalization, we add $\exists x(D(x) \wedge P(x))$*
9. *This completes the proof.*

In this example, it is crucial that we first add $S(a) \wedge D(a)$, and only then claim that $S(a) \Rightarrow P(a)$. This is because in the first step, we use the existence of such a student in order to consider the student explicitly. We are then able to claim that $S(a) \Rightarrow P(a)$ because this holds for *every* $x \in A$, and in particular for a. In contrast, were we to first add $S(a) \Rightarrow P(a)$, we would not be able to claim that $S(a) \wedge D(a)$ because there is no basis for a being a student for which $S(a) \wedge D(a)$ holds.

1.8 Normal Forms and Complete Sets of Logical Connectives

Definition 1.13 *A* literal *is a simple proposition or its negation. A* conjunctive clause *is the conjunction of some set of literals; a* disjunctive clause *is the disjunction of some set of literals.*

- *A proposition is in* disjunctive normal form (DNF) *if it is a disjunction of conjunctive clauses. A proposition is in* full disjunctive normal form *if each of its variables appears exactly once in every clause.*
- *A proposition is in* conjunctive normal form (CNF) *if it is a conjunction of disjunctive clauses.*

Example 1.14

1. *The propositions $p \wedge q$, p, $(p \wedge \neg q) \vee (r \wedge s)$ are in DNF.*
2. *The propositions $\neg(p \vee q)$, $p \vee (q \wedge (r \vee s))$ are not in DNF.*
3. *The propositions $p \wedge (\neg q \vee r)$, $(p \vee q) \wedge (\neg p \vee r)$, and $p \vee q$ are in CNF.*

4. *The propositions* $\neg(p \vee q)$, $(p \wedge q) \vee r$ *are not in CNF.*

5. *The propositions* $p \wedge q$ *and* $p \vee q$ *are in both DNF and CNF.*

Theorem 1.15 *For every proposition* P*, there exists a proposition* Q *in disjunctive normal form that is logically equivalent to* P*.*

Proof: If P is a contradiction, then we take Q to be $p \wedge \neg p$ as the equivalent DNF proposition. Else, let $\mathcal{T}$ be the truth table of P and let $p_1, \ldots, p_n$ be the simple propositions in P. First, remove all rows of $\mathcal{T}$ that have truth value F. Then, for every other row, construct a conjunctive clause by taking p_i if its truth value is T in that row and by taking $\neg p_i$ if its truth value is F in that row. Finally, let Q be the disjunction of all of these conjunctions. It is clear that Q is in DNF. In addition, it is equivalent to P since any assignment that results in T in $\mathcal{T}$ will satisfy a conjunctive clause in Q which will in turn satisfy the entire Q. Furthermore, any assignment that results in T in Q must satisfy at least one conjunctive clause in Q and thus will provide T in the associated row left in $\mathcal{T}$ after removing all the "F rows". Since $\mathcal{T}$ only has T-rows at this point, this means that the assignment satisfies P. Thus, the propositions are equivalent. This completes the proof. ∎

Example 1.16 *Find the equivalent DNF to the proposition* $p \Rightarrow (q \wedge r)$*. What is the size of the DNF proposition and why is this important?*

Observe that if P is not a contradiction, the DNF proposition constructed is in *full* disjunctive normal form. Thus, we have:

Theorem 1.17 *For every proposition* P *that is not a contradiction, there exists a proposition* Q *in full disjunctive normal form that is logically equivalent to* P*.*

It is also possible to show that there is exactly *one* Q in full DNF (ignoring the order of the clauses and literals) that is logically equivalent to P; we will not prove this here.

We remark that although the above demonstrates that an equivalent DNF exists, it may be exponentially bigger than the original P. This is of important *computationally*; you will encounter these questions next year in your studies.

Theorem 1.18 *For every proposition* P*, there exists a proposition* Q *in conjunctive normal form that is logically equivalent to* P*.*

Proof: Let S be a proposition in DNF that is equivalent to $\neg P$; such a proposition is guaranteed to exist by Theorem 1.15. Then, negate S and apply and De Morgan's law. Observe that by De Morgan's law all conjunctions become disjunctions and vice versa; thus the result is $\neg S$ in CNF. Since S is equivalent to $\neg P$ we have that $\neg S$ is equivalent to P, and it is in CNF, thus completing the proof. ∎

Example 1.19 *Find the equivalent CNF to the proposition* $p \Rightarrow (q \wedge r)$*.*

Complete sets of logical connectives. There are many types of logical connectives. We have seen a few of the most common ones, but in principle every different truth tables on two simple propositions defines a (binary) logical connective. Thus, there are $2^4 = 16$ binary logical connectives. However, as we have seen, all propositions can be written in DNF and CNF. Thus, it is possible to express every proposition using only the logical connectives $\{\neg, \vee, \wedge\}$. Thus, this set is "complete". Formally:

Definition 1.20 *A set* S *of logical connectives is* complete *if every proposition has an equivalent proposition that is comprised only of connectives from* S*.*

As we have seen, $\{\neg, \vee, \wedge\}$ is a complete set, and the proof of this is Theorem 1.15. There are also individual connectives that are complete; these are the NAND ($\uparrow$) and NOR ($\downarrow$) connectives, defined as follows: $p \uparrow q = \neg(p \wedge q)$ and $p \downarrow q = \neg(p \vee q)$.

Theorem 1.21 *The following sets of logical connectives are complete:*

1. $\{\neg, \vee\}$
2. $\{\neg, \wedge\}$
3. $\{\neg, \Rightarrow\}$
4. $\{\uparrow\}$
5. $\{\downarrow\}$

Proof: In order to prove this theorem, it suffices to show that the connectives $\{\neg, \vee, \wedge\}$ can be derived from each of the proposed sets. Regarding $\{\neg, \vee\}$, in order to express $p \wedge q$ it is possible to write $\neg(\neg p \vee \neg q)$ and by De Morgan's laws this is equivalent. Thus, any proposition written using $\{\neg, \vee, \wedge\}$ can be rewritten using $\{\neg, \vee\}$. Using De Morgan again, we can obtain that $\{\neg, \wedge\}$ is also complete. Next, observe that $\neg p \Rightarrow q$ is equivalent to $p \vee q$; thus $\{\neg, \Rightarrow\}$ is also complete.

Regarding NAND: observe that $p \uparrow p$ is equivalent to $\neg p$, and $(p \uparrow q) \uparrow (p \uparrow q)$ is equivalent to $\neg(p \uparrow q)$ which is equivalent to $p \wedge q$. Thus, $\{\neg, \wedge\}$ can be expressed using $\uparrow$ alone, proving that $\uparrow$ is complete. We leave the proof of $\downarrow$ (which is very similar) for an exercise. ■

2 Basic Set Theory

2.1 Basic Definitions

A set is a well-defined collection of objects; every member of a set is called an element. We assume that given a set and an element, it is possible to determine whether or not the element is a member of the set (if the set is finite, then this is certainly the case; if not, then it can be determined by the definition of the set). We denote $a \in A$ to mean that a is an element of the set A, and $a \notin A$ to mean that a is not an element of A. A set cannot contain multiple identical elements; thus $\{a, a\} = \{a\}$ (when considering the fact that the only thing that we know about a set is membership or non-membership, this makes sense since the same element appearing multiple times makes no difference to membership). We denote the empty set $\{\}$ containing no elements by $\emptyset$ (equivalently $\emptyset$ is the set with the property that $\forall x : x \notin \emptyset$).

Sets can be defined by using a single-variable propositional function: $A = \{x \mid P(x)\}$ is the set of all values x for which $P(x)$ is true. Observe that there is some ambiguity as to the universe from which x can come from to start with. This ambiguity can be solved by explicitly writing $A = \{x \in \mathbb{N} \mid P(x)\}$, for example, and is sometimes understood from the context. We denote by $\mathcal{U}$ the universal set, or the set of all elements. Observe that we can also write $A = \{x \in \mathcal{U} \mid x \in \mathbb{N} \wedge P(x)\}$. When we refer to x without denoting which set it comes from, by default we refer to $\mathcal{U}$.

Definition 2.1 *Let A and B be sets.*

1. *A is a* subset *of B, denoted $A \subseteq B$, if for every x, $x \in A \Rightarrow x \in B$.*
2. *A is* equal *to B, denoted $A = B$, if for every x, $x \in A \Leftrightarrow x \in B$.*
3. *A is a* proper subset *of B, denoted $A \subset B$ if $A \subseteq B$ and $A \neq B$.*

Basic properties:

1. For every set A, it holds that $A \subseteq A$ and $A = A$
2. If $A = B$ then $B = A$
3. If $A = B$ and $B = C$ then $A = C$
4. $A = B$ if and only if $A \subseteq B$ and $B \subseteq A$
5. If $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$ (this is called *transitivity*)
6. For every set A, $\emptyset \subseteq A$

The above properties should be formally proven. We will give one proof as an example of how to do this, and leave the rest for an exercise.

Theorem 2.2 *If $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$.*

Proof: Let x be an element. Then, $A \subseteq B$ implies that $x \in A \Rightarrow x \in B$. In addition, Since $B \subseteq C$, this implies that $x \in B \Rightarrow x \in C$. By hypothetical syllogism, we have that $x \in A \Rightarrow x \in C$. We have proven this for every arbitrary x, and thus by universal generalization, we have that $\forall x : (x \in A \Rightarrow x \in C)$ and so $A \subseteq C$. ∎

The cardinality of a set A, denoted $|A|$, is the number of (distinct) elements which it contains. If A is an infinite set, then we write $|A| = \infty$.

2.2 Operations on Sets

Definition 2.3

1. Union: *The* union *of two sets A and B, denoted $A \cup B$, is defined by* $\{x \in \mathcal{U} \mid x \in A \vee x \in B\}$
2. Intersection: *The* intersection *of two sets A and B, denoted $A \cap B$, is defined by* $\{x \in \mathcal{U} \mid x \in A \wedge x \in B\}$
3. Complement: *The* complement *of a set A, denoted $\overline{A}$, is defined by* $\{x \in \mathcal{U} \mid x \notin A\}$
4. Difference: *The* set difference *of A and B, denoted $A \setminus B$, is defined by* $\{x \in \mathcal{U} \mid x \in A \wedge x \notin B\}$
5. Symmetric difference: *The* symmetric difference *of A and B, denoted $A \triangle B$, is defined by* $(A \setminus B) \cup (B \setminus A)$

Basic property of union/intersection: For all sets A and B, $A \subseteq A \cup B$ and $A \cap B \subseteq A$.

Equivalence rules of sets:

Idempotent laws:

$$\begin{aligned} A \cap A &= A \\ A \cup A &= A \end{aligned}$$

Commutative laws:

$$\begin{aligned} A \cap B &= B \cap A \\ A \cup B &= B \cup A \end{aligned}$$

Absorption laws:

$$\begin{aligned} A \cap (A \cup B) &= A \\ A \cup (A \cap B) &= A \end{aligned}$$

Associative laws:

$$\begin{aligned} (A \cap B) \cap C &= A \cap (B \cap C) \\ (A \cup B) \cup C &= A \cup (B \cup C) \end{aligned}$$

Distributive laws:

$$\begin{aligned} A \cap (B \cup C) &= (A \cap B) \cup (A \cap C) \\ A \cup (B \cap C) &= (A \cup B) \cap (A \cup C) \end{aligned}$$

Involution law:

$$\overline{\overline{A}} = A$$

De Morgan's laws:

$$\begin{aligned} \overline{(A \cup B)} &= \overline{A} \cap \overline{B} \\ \overline{(A \cap B)} &= \overline{A} \cup \overline{B} \end{aligned}$$

Identity laws:

$$\begin{aligned} A \cup \emptyset &= A \\ A \cap \mathcal{U} &= A \\ A \cup \mathcal{U} &= \mathcal{U} \\ A \cap \emptyset &= \emptyset \end{aligned}$$

Complement laws:

$$\begin{aligned} A \cup \overline{A} &= \mathcal{U} \\ A \cap \overline{A} &= \emptyset \\ \overline{\emptyset} &= \mathcal{U} \\ \overline{\mathcal{U}} &= \emptyset \end{aligned}$$

We will prove one of the rules as an example.

Theorem 2.4 $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Proof: We write the proof as a logical progression. Let x be an arbitrary value. Then,

$$\begin{aligned} x \in A \cap (B \cup C) &\Leftrightarrow x \in A \wedge x \in B \cup C \\ &\Leftrightarrow x \in A \wedge (x \in B \vee x \in C) \\ &\Leftrightarrow (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C) \\ &\Leftrightarrow x \in A \cap B \vee x \in A \cap C \\ &\Leftrightarrow x \in (A \cap B) \cup (A \cap C) \end{aligned}$$

where the third equivalence is obtained by applying the distributive law of logic (Section 1.5). We have proven the above for an arbitrary x, and thus it holds for all x (by universal generalisation). Thus, we conclude that for *every* x, $x \in A \cap (B \cup C) \Leftrightarrow x \in (A \cap B) \cup (A \cap C)$, and so $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. ■

We prove another claim, in order to demonstrate the use of basic logic inference in order to prove statements about set theory.

Theorem 2.5 $A \triangle B = (A \cup B) \setminus (A \cap B)$.

Proof: By definition, $A \triangle B = (A \setminus B) \cup (B \setminus A)$. Let x be an arbitrary value. We have:

$$\begin{aligned} x \in (A \setminus B) \cup (B \setminus A) &\Leftrightarrow (x \in A \setminus B) \vee (x \in B \setminus A) \\ &\Leftrightarrow (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A) \\ &\Leftrightarrow ((x \in A \wedge x \notin B) \vee x \in B) \wedge ((x \in A \wedge x \notin B) \vee x \notin A) \\ &\Leftrightarrow (x \in A \vee x \in B) \wedge (x \in B \vee x \notin B) \wedge (x \in B \vee x \notin B) \wedge (x \notin A \vee x \notin B) \\ &\Leftrightarrow (x \in A \vee x \in B) \wedge (x \notin A \vee x \notin B) \\ &\Leftrightarrow (x \in A \vee x \in B) \wedge (\neg(x \in A) \vee \neg(x \in B)) \\ &\Leftrightarrow (x \in A \vee x \in B) \wedge \neg(x \in A \wedge x \in B) \\ &\Leftrightarrow (x \in A \cup B) \wedge \neg(x \in A \cap B) \\ &\Leftrightarrow (x \in A \cup B) \wedge (x \notin A \cap B) \\ &\Leftrightarrow x \in (A \cup B) \setminus (A \cap B) \end{aligned}$$

We have proven the above for an arbitrary x and thus it holds for every x, proving that $(A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$. We note that the 3rd and 4th equivalence are due to distributivity. In addition, we stress that when using $\notin$ one must be careful. Specifically, it is *not* true that $x \notin A \vee x \notin B$ implies that $x \notin A \cup B$; see above! ■

Operations on many sets: It is possible to define operations on more than sets as well. We define:

$$\begin{aligned}\bigcap_{i=1}^{n} A_i &= A_1 \cap A_2 \cap \cdots \cap A_n = \{x \mid \forall i \in [n] : x \in A_i\} \\ \bigcup_{i=1}^{n} A_i &= A_1 \cup A_2 \cup \cdots \cup A_n = \{x \mid \exists i \in [n] : x \in A_i\}\end{aligned}$$

where $[n]$ denotes the set $\{1, \ldots, n\}$. It is possible to also define this for an arbitrary indexing set I, in which case we have $\bigcap_{i \in I} A_i = \{x \mid \forall i \in I : x \in A_i\}$.

The above can also be defined on *families* of sets (i.e., sets of sets). Specifically, let $\mathcal{F}$ be a set of sets. Then, we denote by $\cap\mathcal{F}$ the intersection of all sets in $\mathcal{F}$, and by $\cup\mathcal{F}$ the union of all sets in $\mathcal{F}$. For example, letting $\mathcal{F} = \{\{1,2\},\{2\},\{2,3,4\}\}$, we have that $\cap\mathcal{F} = \{2\}$ and $\cup\mathcal{F} = \{1,2,3,4\}$.

The power set: The power set of a set A is the set of all subsets of A. Formally, $\mathcal{P}(A) = \{B \mid B \subseteq A\}$. Note that $\mathcal{P}(\emptyset) = \{\emptyset\}$, which is not the same as $\emptyset$ itself ($\mathcal{P}(\emptyset)$ is a set with one element, whereas $\emptyset$ has no elements).

Theorem 2.6 *For all sets A and B:*

1. *$A \subseteq B$ if and only if $\mathcal{P}(A) \subseteq \mathcal{P}(B)$*
2. *$\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B)$*
3. *$\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$*

Proof: We begin with the first statement. First assume that $A \subseteq B$. Assume $X \in \mathcal{P}(A)$. We have:

$$X \in \mathcal{P}(A) \quad \Leftrightarrow \quad X \subseteq A \quad \Rightarrow \quad X \subseteq B \quad \Leftrightarrow \quad X \in \mathcal{P}(B),$$

where the implication "$X \subseteq A \Rightarrow X \subseteq B$" follows from the fact that $A \subseteq B$ (and transitivity of $\subseteq$). Thus, $X \in \mathcal{P}(B)$, and by universal generalization we conclude that $\forall X : X \in \mathcal{P}(A) \Rightarrow X \in \mathcal{P}(B)$ and so $\mathcal{P}(A) \subseteq \mathcal{P}(B)$. For the other direction, we assume that $\mathcal{P}(A) \subseteq \mathcal{P}(B)$ and wish to prove that $A \subseteq B$. Now, by the definition of the power set we have that $A \in \mathcal{P}(A)$. Since $\mathcal{P}(A) \subseteq \mathcal{P}(B)$ and by transitivity we have that $A \in \mathcal{P}(B)$. Again, by the definition of the power set, this implies that $A \subseteq B$, as required.

The second statement is proven as follows:

$$\begin{aligned}X \in \mathcal{P}(A) \cap \mathcal{P}(B) &\Leftrightarrow X \in \mathcal{P}(A) \wedge X \in \mathcal{P}(B) \\ &\Leftrightarrow X \subseteq A \wedge X \subseteq B \\ &\Leftrightarrow X \subseteq A \cap B \\ &\Leftrightarrow X \in \mathcal{P}(A \cap B)\end{aligned}$$

where the third equivalence is proven as follows. Let X be a set and assume that $X \subseteq A$ and $X \subseteq B$. This means that $(\forall x : x \in X \Rightarrow x \in A) \wedge (\forall x : x \in X \Rightarrow x \in B)$. Let a be an arbitrary element. If $a \in X$ then by the above we have that $a \in A$ and $a \in B$, and thus $a \in A \cap B$. By universal generalization, we have that $\forall x : x \in X \Rightarrow x \in A \cap B$. Thus, $X \subseteq A \cap B$. For the other direction, let X be a set and assume $X \subseteq A \cap B$. Since $A \cap B \subseteq A$ and $A \cap B \subseteq B$ (and using the transitivity of intersection; basic property of union/intersection above), we conclude that $X \subseteq A$ and $X \subseteq B$. Thus, $\mathcal{P}(A) \cap \mathcal{P}(B) = \mathcal{P}(A \cap B)$. We stress that it is necessary to prove all unproven claims, including the third equivalence even though it may seem trivial. This will become apparent below since an analogous claim about the union is *not* true.

Regarding the third statement:

$$\begin{aligned}X \in \mathcal{P}(A) \cup \mathcal{P}(B) &\Leftrightarrow X \in \mathcal{P}(A) \vee X \in \mathcal{P}(B) \\ &\Leftrightarrow X \subseteq A \vee X \subseteq B \\ &\Rightarrow X \subseteq A \cup B \\ &\Leftrightarrow X \in \mathcal{P}(A \cup B)\end{aligned}$$

where the implications in third step follows from the fact that $A \subseteq A \cup B$ and $B \subseteq A \cup B$ (prove as exercise) and then apply transitivity (basic property of union/intersection above). Thus, $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$. Observe that one has to be very careful here. It is an "easy mistake" to write all of the steps as "if and only if". However, if $X \subseteq A \cup B$ this does *not* imply that X is a subset of either A or B. For example, take $A = \{1, 2\}$, $B = \{3, 4\}$ and $X = \{2, 3\}$. ∎

It is instructive to look at the lower logic level in an attempt to prove the statement

$$X \subseteq A \vee X \subseteq B \Leftrightarrow X \subseteq A \cup B.$$

In the $\Rightarrow$ direction, we have $X \subseteq A \vee X \subseteq B$ implies that $(\forall x : x \in X \Rightarrow x \in A) \vee (\forall x : x \in X \Rightarrow x \in B)$. Since $A \subseteq A \cup B$ and $B \subseteq A \cup B$, this implies that $(\forall x : x \in X \Rightarrow x \in A \cup B) \vee (\forall x : x \in X \Rightarrow x \in A \cup B)$, which implies $\forall x : x \in X \Rightarrow x \in A \cup B$ or equivalently $X \subseteq A \cup B$.

Now, in an attempt to prove the opposite direction, we start with the assumption that $X \subseteq A \cup B$ which implies that $\forall x : x \in X \Rightarrow x \in A \cup B$, which is equivalent to $\forall x : x \in X \Rightarrow x \in A \vee x \in B$. We would like to write that this implies $(\forall x : x \in X \Rightarrow x \in A) \vee (\forall x : x \in X \Rightarrow x \in B)$ and so $X \subseteq A \cup B$. However, it is ***not true that***:

$$\forall x : P(x) \vee Q(x) \equiv (\forall x : P(x)) \vee (\forall x : Q(x)).$$

This becomes clear if we consider the natural numbers $\mathbb{N}$ and the predicate $P(x)$ to mean that P is even, and $Q(x)$ to mean that P is odd. Since all numbers are either even or odd, we have that $\forall x \in \mathbb{N} : P(x) \vee Q(x)$. However, it is clearly not true that all numbers are even or all numbers are odd which would be the equivalent of $(\forall x : P(x)) \vee (\forall x : Q(x))$.

This explains why in our proofs on sets using logical equivalence, we first fix x to be an arbitrary value (and did not work with a $\forall$ quantifier).

We now continue with the material.

Theorem 2.7 *If $|A| = n$ then $|\mathcal{P}(A)| = 2^n$.*

Proof: Let $A = \{a_1, \ldots, a_n\}$. A subset of A is obtained by taking or not taking each a_i. For every element there are two choices, and each choice is independent of all others. Thus, there are 2^n choices overall. The formal proof of this is by induction (to be shown later). ∎

Definition 2.8

- *Sets A and B are* disjoint *if $A \cap B = \emptyset$.*
- *A set (or family) of sets $\{S_i\}_{i \in I}$ is* pairwise disjoint *if for every $i, j \in I$ with $i \neq j$ it holds that S_i and S_j are disjoint.*
- *A* partition *of a set A is a family $\{S_i \mid i \in I\}$ of non-empty pairwise disjoint subsets of A such that $\bigcup_{i \in I} S_i = A$.*

2.3 Basic Counting Methods

We study some basic methods for counting the cardinality of sets.

Theorem 2.9 *If $A_1, \ldots, A_n$ are pairwise disjoint finite sets, then $|\bigcup_{i=1}^{n} A_i| = \sum_{i=1}^{n} |A_i|$.*

There is nothing to prove here. If a family of sets is pairwise disjoint then each element appears exactly once. Thus, the cardinality of the union of the sets is exactly the sum of the cardinalities of the original sets.

Theorem 2.10 (inclusion-exclusion): *If A and B are finite sets, then $|A \cup B| = |A| + |B| - |A \cap B|$.*

Proof: We partition $A \cup B$ into the following pairwise disjoint sets: $A \setminus B$, $A \cap B$ and $B \setminus A$ (to be exact, this is not necessarily a partition since some of the sets may actually be empty). In order to see that this is a "partition", observe first that all pairs are disjoint (exercise), and that the union equals $A \cup B$ (exercise). Thus, by Theorem 2.9 we have that $|A \cup B| = |A \setminus B| + |A \cap B| + |B \setminus A|$. Next, observe that A can be partitioned into $A \setminus B$ and $A \cap B$; likewise B can be partitioned into $B \setminus A$ and $A \cap B$. Thus, $|A| = |A \setminus B| + |A \cap B|$ and $|B| = |B \setminus A| + |A \cap B|$. Combining the above, we have that

$$|A \cup B| = |A \setminus B| + |A \cap B| + |B \setminus A| = |A| + |B \setminus A| = |A| + |B| - |A \cap B|.$$

■

This can be extended to 3 or more sets. The inclusion-exclusion principle for 3 sets is as follows:

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C|.$$

The general case for n sets will be studied later on in the course.

2.4 Russell's Paradox

Although seemingly rigorous, our treatment here is actually not very formal at all. For example, we did not formally define the axiomatic system necessary for working with sets, and we did not prove our theorems relative to those axioms. But, does this make a difference? In this section, we show that it does. In addition to it being interesting in its own right, this serves as a warning that a lack of exact definitions and formulations can lead to real problems.

As we have stated it, a set can be a collection of anything. In particular, a set can be infinite (like the set of natural numbers $\mathbb{N}$) and it can contain sets (like the power set of any set). Thus, we can also define the set B to be the set of *all* sets; i.e., $B = \{S \mid S \subseteq \mathcal{U}\}$. Although this may seem strange, it is perfectly legitimate by our treatment so far. Note that $B \in B$ since B contains all sets, and is itself a set. This is fine. In contrast, $\mathbb{N} \notin \mathbb{N}$, since $\mathbb{N}$ contains only numbers and $\mathbb{N}$ is a set.

Let us consider now the set of all sets that do *not* contain themselves. That is:

$$A = \{S \mid S \notin S\}$$

We now ask whether $A \in A$ or $A \notin A$. Clearly, one of these must hold (A is either an element of A or it is not). Let us analyze these two possible cases:

- *Case 1 – $A \in A$:* since A contains only sets S for which $S \notin S$, this implies that $A \notin A$; a contradiction.
- *Case 2 – $A \notin A$:* since A contains all sets S for which $S \notin S$ it also contains A by the assumption; thus $A \in A$; a contradiction.

Stated differently, we have proven that $A \in A \Leftrightarrow A \notin A$, which is a contradiction.

There are solutions to Russell's paradox, which involve changing the axioms. We will not deal with them in this course.

Ramifications of Russell's paradox. Define the proposition p to be the statement that $A \in A$ (for the set A above). We have actually proven that p is true and that $\neg p$ is true. The proof that p is true is given in "Case 2" (assuming $A \notin A$ yields a contradiction, thus $A \in A$ and so p is true). In addition, the proof that p is not true is given in "Case 1" (assuming $A \in A$ yields a contradiction, thus $A \notin A$ and so p is not true).

Beyond being a contradiction (since it is not possible that p and $\neg p$ are both simultaneously true), this shows that *naive set theory*, which is what we have used until now, is ***inconsistent*** (where a theory is consistent if it does not contain a contradiction).

Clearly, the fact that a theory contains a contradiction means that it is flawed as a basis for proving mathematical theorems. However, the ramifications are actually far greater than this, and it results in something called the *principle of explosion* which means that *everything can be proven true.* In order to see this, assume that we have proven both p and $\neg p$, and let q be *any* statement. Then, consider the following proof:

1. It is a given that p is true and $\neg p$ is true.

2. By addition to p, it follows that $p \vee q$ is true.

3. We have $p \vee q$ and $\neg p$, and thus by disjunctive syllogism we have that q is true.

The above is a prove that for every q, $p \wedge \neg p \vdash q$.

This is devastating and means that *everything is true within this theory.* Stated differently, even if we have a fully rigorous proof of a statement that uses all of the exact rules of logical inference, it actually means nothing about whether the statement is actually true since technically "everything is true" within the theory. Thus, proofs in naive set theory are actually *meaningless* (you can prove that $0 = 1$ and anything else). This explains why Russell's paradox is so devastating.

One of the major goals of mathematics (set out by Hilbert in 1900) was to prove the consistency of the axioms of arithmetic (stated differently, to prove that the logic theory used to prove mathematics is consistent). Unfortunately, in the 1930s Gödel proved two incompleteness theorems that showed this to be impossible. Specifically, Gödel proved two theorems (which we state very very informally). First, he proved that no theory that is rich enough to prove theorems about the natural numbers can be both complete (meaning that all true statements can be proven) and consistent (that no statement along with its converse can be proven true). Second, he proved that no theory that is "rich enough" can prove that it itself is consistent (to be a little more exact: if the theory can prove itself consistent then it is inconsistent). More about these fascinating results can be studied in the course on logic given in the department.

3 Proof Methods

As we have explained, one of the primary aims of this course is to teach students how to prove. In the past, students were supposed to learn how to prove by example: take enough math or computer science theory courses and you will get the idea. Today, there is more of a trend to *explicitly* teach proof methods. We will adopt this trend in this course. I highly recommend reading Chapter 3 of "How to Prove It" by Daniel Velleman for the material we cover in this portion of the course. We will follow his treatment; however there are many more details in the book than we will cover here.

3.1 Basic Proof Strategies

It is important to note that there is no recipe book for writing a proof. In general, you have to look at what you need to prove and just think until "the proof comes out". This takes time and experience, and you will need to spend considerable time in this course in order to gain the experience you need to learn how to prove. Despite this, there are general strategies that are helpful to know and we will present them here.

Incorrect statements and counterexamples: In order to formally *prove* that a statement is incorrect, it suffices to find a single counterexample. This is due to the fact that unlike in English where "every rule has an exception to the rule", in mathematics an exception means that the rule is invalid. Thus, if you are asked to prove that a statement is incorrect, all you need to do is specify the counterexample. For example, consider the statement:

> Let p and q be prime numbers. Then, $|p - q| > 2$.

This statement is incorrect and in order to prove it I just need to say "11 and 13 are prime numbers and 13-11=2". In fact, a pair of primes of this type is called a twin prime, and we have the following conjecture:

> **Conjecture:** There are infinitely many twin primes.

We have many examples of twin primes, and have found huge positive examples. For example, $3756801695685 \cdot 2^{666669} \pm 1$ is a twin prime that was found in 2011; the numbers have over 200,000 digits. It has been shown that there are $808,675,888,577,436$ twin prime pairs below 10^{18}. Thus, we have strong reason to believe that the conjecture is correct. Nevertheless, a single or many positive example is not a proof of a conjecture, and the twin prime theorem remains open. We thus have the following rule: *A single counterexample is enough to disprove a conjecture, but a theorem cannot be proven by giving positive examples* (unless, of course, the theorem states the existence of something and no more).

Proving a theorem: In order to prove a theorem, you have to begin with the assertions in the hypothesis and rigorously draw inferences, essentially adding to the premises, until you reach the conclusion. We saw this idea in a formal way in Section 1.6. In essence, all theorems should be proven in this way. However, in reality it is tedious to write and tedious to read theorems that are proven at this level of detail. Rather, proofs are written using spoken language. However, a proof is only valid if it follows the same rules of rigor: each statement made in the process of the proof must be fully justified (by proving it or referring to a theorem already proven). We stress that even if you are sure that a statement is correct, if it hasn't been proven rigorously from the hypothesis then you cannot use it in your proof.

Proof strategy 1: *To prove a conclusion of the form $P \Rightarrow Q$, assume that P is true and then prove Q.*

This strategy may sound trivial, but it needs to be explained. Assume that you are trying to prove a theorem of the form "Assume A and B; then P implies Q." It is important to understand that you are *not* asked to prove here that Q is true. Rather, you only need to prove that if P is true then Q is true. Thus, the strategy works by adding P to the premises A and B, and then using all three premises A, B and P in order to derive Q.

Example 3.1 *Let a and b be real numbers. Prove that if $0 < a < b$ then $a^2 < b^2$.*

Our initial hypothesis in this example are that a and b are real numbers. The conclusion is that $P \Rightarrow Q$ where P is the statement that $0 < a < b$ and Q is the statement that $a^2 < b^2$. Thus, we begin our proof with two hypotheses: a and b are real numbers, and $0 < a < b$. We can write this as follows.

The initial state is:

Givens	*Goal*
a and b are real numbers	$0 < a < b \Rightarrow a^2 < b^2$

Using strategy 1, we can change the above to:

Givens	*Goal*
a and b are real numbers	$a^2 < b^2$
$0 < a < b$	

We can now compare the inequalities $a < b$ and $a^2 < b^2$. Multiplying the first inequality by a or b does not change the inequality direction since a and b are positive. Thus, $a < b \Rightarrow a^2 < ab$ and $a < b \Rightarrow ab < b^2$. Combining these together we have that $a^2 < ab < b^2$. This can now be written as a proof as follows:

Theorem 3.2 *Let a and b be real numbers. If $0 < a < b$ then $a^2 < b^2$.*

Proof: Let a and b be real numbers and assume that $0 < a < b$. We multiply $a < b$ by a in order to derive that $a^2 < ab$; this holds since $a > 0$ and so the inequality direction does not change. Next, we multiply $a < b$ by b in order to derive that $ab < b^2$; recall that $b > 0$ as well. We therefore conclude that $a^2 < ab < b^2$ and so $a^2 < b^2$. ■

We summarize proof strategy 1 as follows:

Givens	*Goal*
—	$P \Rightarrow Q$
—	

$\downarrow$

Givens	*Goal*
—	Q
—	
P	

Proof strategy 2: *To prove a conclusion of the form $P \Rightarrow Q$, assume that Q is false and then prove that P is false.*

The basis behind this strategy is the equivalence that we have seen between the statements $P \Rightarrow Q$ and $\neg Q \Rightarrow \neg P$. Note that the statement $\neg Q \Rightarrow \neg P$ is called the contrapositive of $P \Rightarrow Q$. Using the outline above, this strategy works as follows.

Givens	*Goal*
—	$P \Rightarrow Q$
—	

$\downarrow$

Givens	*Goal*
—	$\neg P$
—	
$\neg Q$	

Example 3.3 *Let a, b and c be real numbers and assume that $a > b$. Prove that if $ac \leq bc$ then $c \leq 0$.*

In order to prove this theorem using the contrapositive, we will assume that $c > 0$ and then will show that this implies that $ac > bc$ which is "$\neg P$".

Theorem 3.4 *Let a, b and c be real numbers and assume that $a > b$. If $ac \leq bc$ then $c \leq 0$.*

Proof: We use the strategy and prove the contrapositive. Assume that $c > 0$. Then, c is positive and so we can multiply a and b by c and conclude that $ac > bc$ (based on the assumption that $a > b$). Thus, if $ac \leq bc$ then $c \leq 0$. ∎

3.2 Proofs Involving Negations and Conditionals

Proof strategy 3: *To prove a goal of the form $\neg P$, reexpress the goal in another form and use a strategy for that form.*

This is best demonstrated by an example.

Example 3.5 *Assume that $A \cap C \subseteq B$ and $a \in C$. Prove that $a \notin A \setminus B$.*

Looking at this example, it is not clear at all how to proceed. All we are given is that $a \in C$ and $A \cap C \subseteq B$. We thus begin by changing the form of the goal which is a negation (i.e., currently the goal is that a is *not* in $A \setminus B$).

Now $a \notin A \setminus B$ is equivalent to $\neg(a \in A \wedge a \notin B)$ which is equivalent to $a \notin A \vee a \in B$ (De Morgan) which is equivalent to $a \in A \Rightarrow a \in B$ (conditional law). We therefore have:

Givens	*Goal*
$A \cap C \subseteq B$	$a \in A \Rightarrow a \in B$
$a \in C$	

Applying proof strategy 1 we have:

Givens	*Goal*
$A \cap C \subseteq B$	$a \in B$
$a \in C$	
$a \in A$	

Looking at the above the proof is now trivial. This is because $a \in A$ and $a \in C$ implies that $a \in A \cap C$. Next, since $A \cap C \subseteq B$ this implies that $a \in B$, as required.

Theorem 3.6 *Assume that $A \cap C \subseteq B$ and $a \in C$. Then, $a \notin A \setminus B$.*

Proof: Assume that $a \in A$. Then, since $a \in C$ it follows that $a \in A \cap C$. This in turn implies that $a \in B$ because $A \cap C \subseteq B$. Thus, it cannot be the case that $a \in A$ and $a \notin B$, implying that $a \notin A \setminus B$. ∎

It is not always possible, or natural, to reframe a goal $\neg P$ in a positive form. A common proof strategy to use in such a case is *proof by contradiction*. According to this strategy, you assume that P holds and show that this implies something that is known to be false. Thus, it must be that your initial assumption was incorrect, and so $\neg P$ holds.

Proof strategy 4: *To prove a goal of the form $\neg P$, assume P is true and derive a contradiction.*

Givens	*Goal*
—	$\neg P$
—	

↓

Givens	*Goal*
—	Contradiction
—	
P	

Example 3.7 *Prove that if $x^2 + y = 13$ and $y \neq 4$ then $x \neq 3$.*

Proof: Using the above strategy, we have givens: $x^2 + y = 13$, $y \neq 4$ and $x = 3$. Plugging $x = 3$ into $x^2 + y = 13$ we have that $9 + y = 13$ and so $y = 4$, which is a contradiction to the assumption that $y \neq 4$. Thus, $x \neq 3$. ∎

We remark that many people overuse the proof by contradiction strategy. It is preferable not to use it when a direct proof can be made to work. We now proceed to a strategy that is useful when proving by contradiction.

Proof strategy 5: *To use a* given *of the form $\neg Q$ in order to carry out a proof by contradiction, try to make Q your goal and prove it. This yields a contradiction since Q contradicts the given $\neg Q$.*

Givens	*Goal*
$\neg Q$	Contradiction
—	

↓

Givens	*Goal*
$\neg Q$	Q
—	

This strategy is exactly what we used in the previous example. Essentially, we made it our goal to prove that $y = 4$, which contradicts the given that $y \neq 4$. We now present another example of this.

Example 3.8 *Let A, B and C be sets, and let x be anything. Assume that $A \setminus B \subseteq C$. Prove that if $x \in A \setminus C$ then $x \in B$.*

Proof: Our proof proceeds by showing that if $x \notin B$ then $x \in C$. This contradicts the given that $x \in A \setminus C$ which in particular implies that $x \notin C$.

Let x be an arbitrary element and assume that $x \in A \setminus C$; this implies that $x \in A$ and $x \notin C$. Assume that $x \notin B$. It follows that $x \in A$ and $x \notin B$ which implies that $x \in A \setminus B$. Applying the given that $A \setminus B \subseteq C$ we have that $x \in C$. This contradicts the given that $x \notin C$, and so we conclude that $x \in B$. ∎

We stress that the above proof is facilitated by our familiarity with the exact definitions of set difference. It is impossible to prove theorems without a complete understanding of the material being studied.

Next, we present a strategy for using a given of the form $\neg Q$ in a proof that is not a proof by contradiction.

Proof strategy 6: *To use a* given *of the form $\neg P$, reexpress the given in a different form.*

This strategy can be used in the same way as strategy 3, except that here it relates to a given and not a goal. We therefore do not give another example of how to use this. We now proceed to strategies that relate to givens of the form $P \Rightarrow Q$ (so far we have only see strategies for goals of this form).

Proof strategy 7: *To use a* given *of the form $P \Rightarrow Q$: prove that P is true and conclude that Q is true, or prove that Q is false and conclude that P is false.*

The first part of the above strategy is the "modus ponens" rule of inference that we saw in Section 1.6; the second part is the "modus tollens" rule of inference.

Example 3.9 *Assume that $P \Rightarrow (Q \Rightarrow R)$. Prove that $\neg R \Rightarrow (P \Rightarrow \neg Q)$.*

We prove this using the proof strategies, although it would be more easily proven by just constructing a truth table. Observe, that it is not immediately obvious how to proceed with this proof. According to modus ponens, if we knew P then we could add $Q \Rightarrow R$ to our givens; likewise, according to modus tollens, if we knew $\neg(Q \Rightarrow R)$ then we could add $\neg P$ to our givens. However, neither of these is known. Thus, we make our first goal to prove either P or $\neg(Q \Rightarrow R)$. We begin by writing our givens and goal, and proceeding step by step using our strategies:

Givens	*Goal*
$P \Rightarrow (Q \Rightarrow R)$	$\neg R \Rightarrow (P \Rightarrow \neg Q)$

$\downarrow$ Using strategy 1

Givens	*Goal*
$P \Rightarrow (Q \Rightarrow R)$	$P \Rightarrow \neg Q$
$\neg R$	

$\downarrow$ Using strategy 1

Givens	*Goal*
$P \Rightarrow (Q \Rightarrow R)$	$\neg Q$
$\neg R$	
P	

$\downarrow$ Using modus ponens

Givens	*Goal*
$P \Rightarrow (Q \Rightarrow R)$	$\neg Q$
$\neg R$	
P	
$Q \Rightarrow R$	

Observe now that we have $\neg R$ and $Q \Rightarrow R$ as givens. Thus, by modus tollens it holds that $\neg Q$, and so the proof is complete. The above is an example of strategy 7 since although we are applying strategy 1 and modus ponens, the overall aim is to use the given implication, and in order to do so we have to somehow "prove" the premise of it. This "proof" is actually achieved by applying strategy 1 (essentially, assuming that P is true is a proof of it within the context of what we need to prove; beware, however, that you can only do this if you are asked to prove an implication and so can apply strategy 1).

Theorem 3.10 *Assume that $P \Rightarrow (Q \Rightarrow R)$. Then, $\neg R \Rightarrow (P \Rightarrow \neg Q)$.*

Proof: Assume $\neg R$, and assume P. Since $P \Rightarrow (Q \Rightarrow R)$, we have that $Q \Rightarrow R$. However, by $\neg R$, it follows that $\neg Q$. Thus, $P \Rightarrow \neg Q$. We conclude that $\neg R \Rightarrow (P \Rightarrow \neg Q)$. ■

Example 3.11 *Assume that $A \subseteq B$, $a \in A$ and $a \notin B \setminus C$. Prove that $a \in C$.*

Givens	*Goal*
$A \subseteq B$	$a \in C$
$a \in A$	
$a \notin B \setminus C$	

↓ Using strategy 6

Givens	*Goal*
$A \subseteq B$	$a \in C$
$a \in A$	
$a \notin B \vee a \in C$	

↓ Material implication law

Givens	*Goal*
$A \subseteq B$	$a \in C$
$a \in A$	
$a \in B \Rightarrow a \in C$	

↓ Change goal using modus ponens (strategy 7)

Givens	*Goal*
$A \subseteq B$	$a \in B$
$a \in A$	

Now, since $A \subseteq B$ and $a \in A$, it follows that $a \in B$. Thus, our goal can be reached.

Theorem 3.12 *If $A \subseteq B$, $a \in A$ and $a \notin B \setminus C$, then $a \in C$.*

Proof: Since $a \in A$ and $A \subseteq B$ it follows that $a \in B$. But $a \notin B \setminus C$ and thus $a \in C$, as required. ∎

3.3 Proofs Involving Quantifiers

Proof strategy 8: *To prove a goal of the form $\forall x P(x)$, let x stand for an arbitrary object and prove $P(x)$.*

We have seen this proof strategy multiple times; one case is in Example 3.8. The idea behind this strategy is that specifying x gives you something concrete to analyze. We will present the next example briefly.

Example 3.13 *Assume that A, B and C are sets. If $A \setminus B \subseteq C$ then $A \setminus C \subseteq B$.*

Proof: Let x be an arbitrary value, and assume that $x \in A \setminus C$. This implies that $x \in A$ and $x \notin C$. If $x \notin B$, then $x \in A \setminus B$ and by the fact that $A \setminus B \subseteq C$ it follows that $x \in C$, which is a contradiction. We have shown that for every arbitrary x, if $x \in A \setminus C$ then $x \in B$, and thus $A \setminus C \subseteq B$. ∎

Proof strategy 9: *To prove a goal of the form $\exists x P(x)$, find a value x for which $P(x)$ is true and prove this. Make sure that x is a new variable.*

Example 3.14 *Prove that for every real number x, if $x > 0$ then there exists a real number y such that $y(y+1) = x$.*

In order to find such a y, we can work backwards. Specifically:

$$y(y+1) = x \Rightarrow y^2 + y - x = 0 \Rightarrow y = \frac{-1 \pm \sqrt{1+4x}}{2}.$$

According to the strategy, this work need not appear in the proof.

Theorem 3.15 *Prove that for every real number x, if $x > 0$ then there exists a real number y such that $y(y+1) = x$.*

Proof: Let x be an arbitrary real number and assume that $x > 0$. Let $y_0 = \frac{-1+\sqrt{1+4x}}{2}$. First observe that since x is positive, $\sqrt{1+4x}$ is a real number and so y_0 is a real number. Next,

$$y_0(y_0+1) = \frac{-1+\sqrt{1+4x}}{2} \cdot \frac{1+\sqrt{1+4x}}{2} = \frac{(1+4x)-1}{4} = x.$$

This completes the proof. ■

The above strategy relates to a goal of the form $\exists x P(x)$. We will now consider how to work with a given of the form $\exists x P(x)$. Note that in this case we don't necessarily know of any concrete example for which $P(x)$ holds; we just know that such an x does exist. The next strategy states that in such a case it is helpful to give the x that is guaranteed to exist a concrete name, like x_0. This strategy is called existential instantiation in logic.

Proof strategy 10: *To use a given of the form $\exists x P(x)$, introduce a new variable x_0 and assume that $P(x_0)$ is true.*

In the case of a given of the form $\forall x P(x)$, it is possible to plug in *any* value in place of x. The next strategy says exactly this. However, we stress that it is typically only useful when you have a concrete value a for which it is useful to claim that $P(a)$ is true. This strategy is called universal instantiation in logic.

Proof strategy 11: *To use a given of the form $\forall x P(x)$, plug in any a you wish and conclude that $P(a)$ is true.*

We have actually already used this strategy. Specifically, in Example 3.12, we start by saying that since $a \in A$ and $A \subseteq B$ it follows that $a \in B$. Observe that $A \subseteq B$ is actually a given of the form $\forall x : x \in A \Rightarrow x \in B$. Then, once we take $a \in A$, we can plug it into the given and conclude that $a \in B$.

In the next example, we will refer to *families* of sets. We remark that these are just sets of sets, and so operations like intersection and union are well defined. For a family of sets $\mathcal{F}$, we denote

$$\cap\mathcal{F} = \bigcap_{A\in\mathcal{F}} A \quad \text{and} \quad \cup\mathcal{F} = \bigcup_{A\in\mathcal{F}} A$$

Example 3.16 *Assume that $\mathcal{F}$ and $\mathcal{G}$ are families of sets, and $\mathcal{F} \cap \mathcal{G} \neq \emptyset$. Prove that $\cap\mathcal{F} \subseteq \cup\mathcal{G}$.*

This example is a bit confusing and the first step is understand the intuition behind the statement. This can be achieved by first writing the statement in its logical form: $\forall x(x \in \cap\mathcal{F} \Rightarrow x \in \cup\mathcal{G})$. Now, intuitively, if $\mathcal{F} \cap \mathcal{G} \neq \emptyset$ then there exist some sets in their intersection. Any value $x \in \cap\mathcal{F}$ is in all of the sets of $\mathcal{F}$. Thus, it is in all the sets in the intersection $\mathcal{F} \cap \mathcal{G}$. This suffices since we can conclude that x is in some set in $\mathcal{G}$ and so it is in $\cup\mathcal{G}$. Having understood the intuition, we can proceed to constructing a rigorous proof.

Givens	*Goal*
$\mathcal{F} \cap \mathcal{G} \neq \emptyset$	$x \in \cup\mathcal{G}$
$x \in \cap\mathcal{F}$	

↓ Rewrite in the logical forms

Givens	*Goal*
$\exists A(A \in \mathcal{F} \cap \mathcal{G})$	$\exists A \in \mathcal{G}(x \in A)$
$\forall A \in \mathcal{F}(x \in A)$	

↓ Using strategy 10

Givens	*Goal*
$A_0 \in \mathcal{F}$	$\exists A \in \mathcal{G}(x \in A)$
$A_0 \in \mathcal{G}$	
$\forall A \in \mathcal{F}(x \in A)$	

↓ Using strategy 11

Givens	*Goal*
$A_0 \in \mathcal{F}$	$\exists A \in \mathcal{G}(x \in A)$
$A_0 \in \mathcal{G}$	
$x \in A_0$	

This suffices to prove the theorem since $A_0 \in G$ and $x \in A_0$. We now write out the actual proof.

Theorem 3.17 *Assume that $\mathcal{F}$ and $\mathcal{G}$ are families of sets, and $\mathcal{F} \cap \mathcal{G} \neq \emptyset$. Then, $\cap\mathcal{F} \subseteq \cup\mathcal{G}$.*

Proof: Let x be an arbitrary element and assume that $x \in \cap\mathcal{F}$. Since $\mathcal{F} \cap \mathcal{G} \neq \emptyset$ there exists a set A_0 that is an element of $\mathcal{F} \cap \mathcal{G}$, implying that $A_0 \in \mathcal{F}$ and $A_0 \in \mathcal{G}$. Since $x \in \cap\mathcal{F}$ it follows that $x \in A_0$. However, since $A_0 \in \mathcal{G}$ as well, we have that $x \in \cup\mathcal{G}$. We have shown that $\forall x(x \in \cap\mathcal{F} \Rightarrow x \in \cup\mathcal{G})$ and so $\cap\mathcal{F} \subseteq \cup\mathcal{G}$. ■

In the previous proof, there are three types of objects: families of sets ($\mathcal{F}$ and $\mathcal{G}$), sets (A_0), and elements (x). It is important to always be explicit regarding the type of entity introduced. In addition, it is important to be explicit as to whether a value x is quantified so that it refers to a specific object, or quantified universally. We present another example.

Example 3.18 *Assume that B is a set and that $\mathcal{F}$ is a family of sets. Prove that if $\cup\mathcal{F} \subseteq B$ then $\mathcal{F} \subseteq \mathcal{P}(B)$.*

As before, it is important to first obtain intuition. This case is actually quite easy. If $\cup\mathcal{F} \subseteq B$ then all of the elements in $\cup\mathcal{F}$ appear in B and so the power set of B contains all of the possible subsets containing these elements. Since $\mathcal{F}$ contains some family of sets of these elements, it is a subset of $\mathcal{P}(B)$. We now proceed to the construct the proof.

Givens	*Goal*
$\cup\mathcal{F} \subseteq B$	$\mathcal{F} \subseteq \mathcal{P}(B)$

↓ Rewrite in the logical form

Givens	*Goal*
$\cup\mathcal{F} \subseteq B$	$\forall x(x \in \mathcal{F} \Rightarrow x \in \mathcal{P}(B))$

↓ Using strategies 1 and 8

Givens	*Goal*
$\cup\mathcal{F} \subseteq B$	$x \in \mathcal{P}(B)$
$x \in \mathcal{F}$	

↓ Using logical form of $x \in \mathcal{P}(B)$: $\forall y(y \in x \Rightarrow y \in B)$

Givens	*Goal*
$\cup\mathcal{F} \subseteq B$	$y \in B$
$x \in \mathcal{F}$	
$y \in x$	

↓ Change notation to prevent confusion between elements and sets

Givens	*Goal*
$\cup\mathcal{F} \subseteq B$	$y \in B$
$A \in \mathcal{F}$	
$y \in A$	

↓ Using strategy 7

Givens	*Goal*
$\cup\mathcal{F} \subseteq B$	$y \in \cup\mathcal{F}$
$A \in \mathcal{F}$	
$y \in A$	

This completes the proof since $y \in A$ and $A \in \mathcal{F}$; thus $y \in \cup\mathcal{F}$. (We note that the last step is by strategy 7 since $\cup\mathcal{F} \subseteq B$ is actually $y \in \cup\mathcal{F} \Rightarrow y \in B$ and so we use this given to replace the goal of $y \in B$ with $y \in \cup\mathcal{F}$).

Theorem 3.19 *Assume that B is a set and $\mathcal{F}$ is a family of sets. If $\cup\mathcal{F} \subseteq B$ then $\mathcal{F} \subseteq \mathcal{P}(B)$.*

Proof: Assume that $\cup\mathcal{F} \subseteq B$. Let A be an arbitrary element (set) and assume that $A \in \mathcal{F}$, and let y be an arbitrary element and assume that $y \in A$. Since $y \in A$ and $A \in \mathcal{F}$ it follows that $y \in \cup\mathcal{F}$. By the fact that $\cup\mathcal{F} \subseteq B$, it follows that $y \in B$. Thus, $\forall y(y \in A \Rightarrow y \in B)$ and so $A \subseteq B$. By the definition of $\mathcal{P}(B)$ this implies that $A \in \mathcal{P}(B)$. We have proven that $\forall A(A \in \mathcal{F} \Rightarrow A \in \mathcal{P}(B))$ and so $\mathcal{F} \subseteq \mathcal{P}(B)$. ∎

3.4 Proofs Involving Conjunctions and Biconditionals

The first two strategies for conjunctions are trivial.

Proof strategy 12: *To prove a goal of the form $P \wedge Q$, prove P and Q separately.*

Proof strategy 13: *To use a given of the form $P \wedge Q$, treat P and Q as two separate givens.*

We have seen this strategy in the past. For example, in Example 3.8, we take the fact that $x \in A \setminus C$ and use the two given $x \in A$ and $x \notin C$. Observe that in that proof, we use the fact that $x \in A$ in a completely separate place from the fact that $x \notin C$. The next two strategies are also very straightforward.

Proof strategy 14: *To prove a goal of the form $P \Leftrightarrow Q$, prove $P \Rightarrow Q$ and $Q \Rightarrow P$ separately.*

Proof strategy 15: *To use a given of the form $P \Leftrightarrow Q$, treat $P \Rightarrow Q$ and $Q \Rightarrow P$ as two separate givens.*

In order to illustrate these strategies, we provide a very simple example. Specifically, we wish to prove that x is even if and only if x^2 is even. According to strategy 14, we prove each direction separately. The direction that if x is even then x^2 is even is very easy, as long as you use existential instantiation (strategy 10) to give you a handle on the values. Specifically, using strategy 10, if x is even then $x = 2k$ for some k. It is then trivial to see that $x^2 = 4k^2$ is also even. For the other direction, we can start by assuming that x^2 is even and prove that x is even. However, here all we are given is that $x^2 = 2k'$ for some k' and this doesn't seem to be too helpful. Nevertheless, the problem is solved by using strategy 2 (proving the contrapositive). Specifically, if we assume that x is odd, then it is again easy to show that x^2 is odd.

Example 3.20 *Let x be an integer. Then, x is even if and only if x^2 is even.*

Proof: Assume that x is even. Then, $x = 2k$ for some $k \in \mathbb{Z}$. Thus $x^2 = 4k$ and is even. For the reverse direction, assume that x is odd. This implies that $x = 2k' + 1$ for some $k' \in \mathbb{Z}$, and thus $x^2 = 4k'^2 + 4k' + 1$ which is odd. Thus, if x^2 is even then x is even. ∎

Additional examples: We finish this section by proving two theorems that demonstrate what we have seen so far. In Section 1.6 we explained intuitively that the negation of $\forall x P(x)$ is $\exists x \neg P(x)$, and that the negation of $\exists x P(x)$ is $\forall x \neg P(x)$. We will now prove this formally. We begin with the direction that $\forall x \neg P(x) \Rightarrow \neg\exists x P(x)$.

Example 3.21 *Prove that $\forall x \neg P(x)$ if and only if $\neg\exists x P(x)$.*

Givens	*Goal*
$\forall x \neg P(x)$	$\neg \exists x P(x)$

$\downarrow$ Using strategy 4

Givens	*Goal*
$\forall x \neg P(x)$	Contradiction
$\exists x P(x)$	

$\downarrow$ Using strategy 10

Givens	*Goal*
$P(x_0)$	Contradiction
$\forall x \neg P(x)$	

$\downarrow$ Using strategy 11

Givens	*Goal*
$P(x_0)$	Contradiction
$\neg P(x_0)$	

The reverse direction is similar and so we'll proceed to the actual proof.

Theorem 3.22 $(\forall x \neg P(x)) \Leftrightarrow (\neg \exists x P(x))$.

Proof: ($\Rightarrow$): Assume that $\forall x \neg P(x)$ and that $\exists x P(x)$. This implies that for some x_0 it holds that $P(x_0)$ is true. However, since $\forall x \neg P(x)$ it holds that $P(x_0)$ is false. This is a contradiction, and thus $\forall x \neg P(x) \Rightarrow \neg \exists x P(x)$.

($\Leftarrow$): Assume that $\neg \exists x P(x)$, and let x be an arbitrary value. If $P(x)$ is true, then $\exists x P(x)$ which is a contradiction. Thus, $\neg P(x)$. Since x is arbitrary we have shown that $\forall x \neg P(x)$. Thus, $\neg \exists x P(x) \Rightarrow \forall x \neg P(x)$. ■

There are some cases where it is possible to prove both directions at the same time. This occurs when each step of the proof is an "if and only if". We used this proof technique in order to prove Theorem 2.6. In the next example, we will use the technique to prove that $A \cap (B \setminus C) = (A \cap B) \setminus C$. The first step of the proof is to write each expression in its logical form. We write:

$$x \in A \cap (B \setminus C) \quad \Leftrightarrow \quad x \in A \wedge x \in B \setminus C \quad \Leftrightarrow \quad x \in A \wedge x \in B \wedge x \notin C$$

$$x \in (A \cap B) \setminus C \quad \Leftrightarrow \quad x \in A \cap B \wedge x \notin C \quad \Leftrightarrow \quad x \in A \wedge x \in B \wedge x \notin C$$

and it is immediately clear that they are equivalent.

Theorem 3.23 *Let A, B and C be sets. Then $A \cap (B \setminus C) = (A \cap B) \setminus C$.*

Proof: Let x be an arbitrary value. Then:

$$\begin{aligned} x \in A \cap (B \setminus C) &\Leftrightarrow x \in A \wedge x \in B \setminus C \\ &\Leftrightarrow x \in A \wedge x \in B \wedge x \notin C \\ &\Leftrightarrow x \in A \cap B \wedge x \notin C \\ &\Leftrightarrow x \in (A \cap B) \setminus C \end{aligned}$$

Since x is arbitrary, we have proven that $\forall x(x \in A \cap (B \setminus C)) \Leftrightarrow \forall x(x \in (A \cap B) \setminus C)$ and thus $A \cap (B \setminus C) = (A \cap B) \setminus C$. ■

Multiple equivalences: In some cases, you need to prove that $P \Leftrightarrow Q \Leftrightarrow R$ and possibly even more. It is possible to apply strategy 14 four different times in order to prove $P \Leftrightarrow Q$ and $Q \Leftrightarrow R$. However, it suffices to prove that $P \Rightarrow Q$, $Q \Rightarrow R$ and $R \Rightarrow P$, which requires proving only three implications.

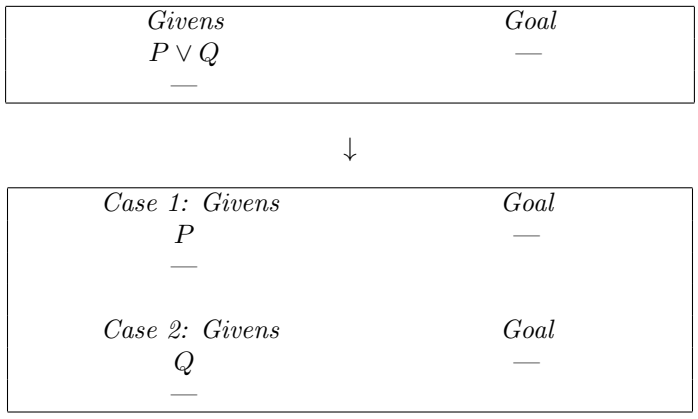
Proof strategy 16: *To prove a goal of the form $P \Leftrightarrow Q \Leftrightarrow R$, separately prove $P \Rightarrow Q$, $Q \Rightarrow R$ and $R \Rightarrow P$.*

Observe also that if you are asked to prove the equivalence of P, Q, R and S, then repeated application of strategy 14 requires proving 6 implications, in contrast to 4 using this strategy.

3.5 Proofs Involving Disjunctions

In some instances, a given or a goal contains a disjunction of the form $P \vee Q$. In this section, we discuss proof strategies for dealing with this situation.

Proof strategy 17: *To use a given of the form $P \vee Q$, break the proof into cases. For case 1, assume that P is true and prove the goal; for case 2, assume that Q is true and prove the goal.*



We now give an example of this strategy. Specifically, we prove that $A \subseteq C$ And $B \subseteq C$ then $A \cup B \subseteq C$. This looks like a case where the givens are a conjunction. However, we first rewrite the goal in its logical form as: $x \in A \cup B \Rightarrow x \in C$, which is equivalent to $(x \in A \vee x \in B) \Rightarrow x \in C$. Now, by proof strategy 1, we can add $x \in A \vee x \in B$ to the givens and modify our goal to $x \in C$. We now have a situation where proof strategy 17 is appropriate.

Theorem 3.24 *Assume that A, B and C are sets. If $A \subseteq C$ and $B \subseteq C$ then $A \cup B \subseteq C$.*

Proof: Assume that $A \subseteq C$ and $B \subseteq C$. Let x be an arbitrary element. If $x \in A \cup B$ then this implies that $x \in A$ or $x \in B$. There are two cases:

- *Case 1 – $x \in A$:* Since $A \subseteq C$ it follows that $x \in C$.
- *Case 2 – $x \in B$:* Since $B \subseteq C$ it follows that $x \in C$.

Since $x \in A$ or $x \in B$, these cases cover all possibilities and so we can conclude that $x \in C$. We have proven that for every x, if $x \in A \cup B$ then $x \in C$, and thus we conclude that $A \cup B \subseteq C$. ∎

There are two important comments to make regarding this proof. First, it is crucial that the cases indeed cover *all* possibilities; otherwise the proof is not valid. Second, it is not necessary that the cases be exclusive. For example, it is possible that an element x is in both A and B. This does not matter. We now proceed to the strategy when the goal is $P \vee Q$.

Proof strategy 18: *To prove a goal of the form $P \vee Q$, either prove P or prove Q.*

Example 3.25 *Assume that A, B and C are sets. Prove that $A \setminus (B \setminus C) \subseteq (A \setminus B) \cup C$.*

Givens	*Goal*
	$x \in A \setminus (B \setminus C) \Rightarrow x \in (A \setminus B) \cup C$

↓ Using strategy 1

Givens	*Goal*
$x \in A \setminus (B \setminus C)$	$x \in (A \setminus B) \cup C$

↓ Writing in logical form

Givens	*Goal*
$x \in A \wedge \neg(x \in B \wedge x \notin C)$	$(x \in A \wedge x \notin B) \vee x \in C$

↓ Using De Morgan

Givens	*Goal*
$x \in A \wedge (x \notin B \vee x \in C)$	$(x \in A \wedge x \notin B) \vee x \in C$

↓ Using strategy 17

Case 1: Givens	*Goal*
$x \in A$	$(x \in A \wedge x \notin B) \vee x \in C$
$x \notin B$	
Case 2: Givens	*Goal*
$x \in A$	$(x \in A \wedge x \notin B) \vee x \in C$
$x \in C$	

↓ Using strategy 18 (and choosing wisely)

Case 1: Givens	*Goal*
$x \in A$	$x \in A \wedge x \notin B$
$x \notin B$	
Case 2: Givens	*Goal*
$x \in A$	$x \in C$
$x \in C$	

Theorem 3.26 *Assume that A, B and C are sets. Then, $A \setminus (B \setminus C) \subseteq (A \setminus B) \cup C$.*

Proof: Let x be be an arbitrary element and assume that $x \in A \setminus (B \setminus C)$. Then, $x \in A$ and $x \notin B \setminus C$. Since $x \notin B \setminus C$, it follows that either $x \notin B$ or $x \in C$. We will consider these cases separately:

- *Case 1 – $x \notin B$:* Since $x \in A$ it follows that $x \in A \setminus B$ and $x \in (A \setminus B) \cup C$.
- *Case 2 – $x \in C$:* Clearly $x \in (A \setminus B) \cup C$.

Since x was an arbitrary element of $A \setminus (B \setminus C)$, we conclude that $A \setminus (B \setminus C) \subseteq (A \setminus B) \cup C$. ■

Proof strategy 19: *To prove a goal of the form $P \vee Q$, if P is true then clearly $P \vee Q$ is true; thus, it suffices to prove that Q is true in the case that P is false.*

Givens	*Goal*
—	$P \vee Q$
—	

$\downarrow$

Case 1: Givens	*Goal*
—	Q
—	
$\neg P$	—

Example 3.27 *Assume that m and n are integers. Prove that if mn is even, then either m is even or n is even.*

Givens	*Goal*
mn is even	m is even or n is even

$\downarrow$ Using strategy 19

Case 1: Givens	*Goal*
mn is even	n is even
m is odd	

Theorem 3.28 *Assume that m and n are integers. If mn is even, then either m is even or n is even.*

Proof: Assume that mn is even; let $k \in \mathbb{Z}$ be such that $mn = 2k$. If m is even, then the theorem clearly holds. Thus, assume that m is odd. This implies that $m = 2j + 1$ for some $j \in \mathbb{Z}$. Plugging this into the equation $mn = 2k$ we have that $2k = (2j + 1) \cdot n = 2jn + n$, and so $n = 2k - 2jn = 2(k - jn)$. Since $k - jn$ is an integer we conclude that n is even. ∎

3.6 Existence and Uniqueness Proofs

In this section, we consider proofs in which the goal is the existence of a *unique* value; that is $\exists! x P(x)$. In logical form, this can be written as $\exists x(P(x) \wedge \neg\exists y(P(y) \wedge y \neq x))$.[1] By strategy 9, it suffices to find a value x such that $P(x)$ is true and $\neg\exists y(P(y) \wedge \neg x)$. This latter statement is a negation, and so by strategy 3 we find an alternate form:

$$\begin{aligned} \neg\exists y(P(y) \wedge y \neq x) &\equiv \forall y \neg(P(y) \wedge y \neq x) && \text{(quantifier negation)} \\ &\equiv \forall y(\neg P(y) \vee y = x) && \text{(De Morgan)} \\ &\equiv \forall y(P(y) \Rightarrow y = x) && \text{(conditional law)} \end{aligned}$$

Thus $\exists! x P(x)$ is equivalent to $\exists x(P(x) \wedge \forall y(P(y) \Rightarrow y = x))$. This final form is actually very intuitive. There exists a *unique* x if there exists some x such that $P(x)$ is true and for every y for which $P(y)$ is true it holds that $y = x$. This may seem a roundabout way of saying that there exists a unique x, but it is actually very useful in proving theorems.

We can even further manipulate this and write $\exists x P(x) \wedge \forall y \forall z((P(y) \wedge P(z)) \Rightarrow y = z)$. This is a better form for writing proofs since there is no common quantifier between the two statements in the conjunction.

[1] By the way, observe the difference between what we wrote and $(\exists x P(x)) \wedge \neg\exists y(P(y) \wedge y \neq x)$. Can you see why the form written here is not valid?

Proof strategy 20: *To prove a goal of the form* $\exists! x P(x)$*, separately prove* $\exists x P(x)$ (existence)*, and* $\forall y \forall z((P(y) \wedge P(z)) \Rightarrow y = z)$ (uniqueness).

Example 3.29 *Prove that there exists a unique set* A *such that for every set* B*,* $A \cup B = B$*.*

As in all such proofs, the first step is to understand the statement and work out which set is the unique set we are looking for. Clearly A cannot add anything new to B, but in fact it cannot add anything new to any set. Thus A must be the empty set. Once we have understood this, we already have our existence part of the proof since indeed $\forall B(\emptyset \cup B = B)$. For uniqueness, we need to prove that for arbitrary C and D it holds that $\forall B(C \cup B = B \wedge D \cup B = B) \Rightarrow C = D$. Specifically,

Givens	*Goal*
$\forall B(C \cup B = B)$	$C = D$
$\forall B(D \cup B = B)$	

In order to use these givens, we have to instantiate B in both cases. Instantiating B with D in the first given gives that $C \cup D = D$, and instantiating B with C in the second given gives that $D \cup C = C$. Thus, $D = C \cup D = D \cup C = C$ and so $C = D$. This proof therefore uses universal instantiation (proof strategy 11).

Theorem 3.30 *There exists a unique set* A *such that for every set* B*,* $A \cup B = B$*.*

Proof: We first prove existence. Take $A = \emptyset$. Then, for every set B, $\emptyset \cup B = B$, as required. We next prove uniqueness. Let C and D be such that $\forall B(C \cup B = B)$ and $\forall B(D \cup B = B)$. Applying the first assumption to D we have that $C \cup D = D$; applying the second assumption to C we have that $D \cup C = C$. Thus, $D = C \cup D = D \cup C = C$, as required. ∎

We conclude with one last proof strategy; the way to use it is similar to the previous strategy.

Proof strategy 21: *To use a given of the form* $\exists! x P(x)$*, add the two givens* $\exists x P(x)$*, and* $\forall y \forall z((P(y) \wedge P(z)) \Rightarrow y = z)$ (uniqueness).

3.7 One Summary Proof

Theorem 3.31 *There an infinite number of prime numbers.*

Proof: Assume, by contradiction, that there only a finite number of primes. Let $p_1, \ldots, p_n$ be a list of all of the prime number, and let $m = p_1 \cdot p_2 \cdots p_n + 1$. Observe that for every $i = 1, \ldots, n$ it holds that p_i does not divide m. This is due to the fact that such a division gives a remainder of 1 always.

Now, every integer larger than 1 is either prime or a product of primes (we will prove this later in the course). Since m is larger than 1, it must be either prime or a product of primes. However, we have already seen that m is not a product of primes since none of the primes in the exhaustive list of primes divides m. Thus m must be prime. However, $m \neq p_i$ for all i; thus m is not one of the primes in the list of all primes. We thus derive a contradiction and we conclude that there must be an infinite number of primes. ∎

Let us analyze the proof steps. First, we apply strategy 4 ("infinite" is actually a negation), and then strategy 10 (existential instantiation) in order to obtain the list $p_1, \ldots, p_n$. From this point on, we work to derive a contradiction by proving that there *exists* a value q such that $q \notin \{p_1, \ldots, p_n\}$ and q is prime. In order to prove this existential claim, we pinpoint an actual value m and prove that it holds for m.

4 Relations

4.1 Ordered Pairs and Cartesian Products

So far we have considered sets, in which the order makes no difference (i.e., $\{a, b\} = \{b, a\}$) and the same element cannot appear twice (i.e., $\{a, a\}$ is not defined). We now wish to define an ordered pair where $(a, b) \neq (b, a)$ and where (a, a) is allowed.

Definition 4.1 *An* ordered pair (a, b) *is the set* $\{\{a\}, \{a, b\}\}$.

We remark that formally one needs to show that (a, a) exists and that $(a, b) = (c, d)$ if and only if $a = c$ and $b = d$. In order to do this, one needs to work formally from the axioms of set theory. We omit this material in this course.

Definition 4.2 *Let A and B be sets. The* cartesian product *of A and B, denoted $A \times B$, is defined by*

$$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}.$$

Theorem 4.3 *Let A, B, C and D be sets. Then,*

1. $A \times (B \cap C) = (A \times B) \cap (A \times C)$
2. $A \times (B \cup C) = (A \times B) \cup (A \times C)$
3. $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$
4. $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$
5. $A \times \emptyset = \emptyset \times A = \emptyset$

Proof: We will prove the 1st, 4th and 5th items (the 2nd and 3rd can be easily derived from the 1st and 4th, proofs).

1. Assume that there exists a $p \in A \times (B \cap C)$; by the definition of the cartesian product $p = (x, y)$ for some $x \in A$ and $y \in B \cap C$. Thus, $y \in B$ and $y \in C$, implying that $p = (x, y) \in A \times B$ and $p = (x, y) = A \times C$, and so $p \in (A \times B) \cap (A \times C)$. Since p was an arbitrary element, we have that $A \times (B \cap C) \subseteq (A \times B) \cap (A \times C)$. For the other direction, assume that there exists a $p \in (A \times B) \cap (A \times C)$; this implies that $p = (x, y)$ for some $(x, y) \in A \times B$ and $(x, y) \in A \times C$. Thus, $x \in A$. In addition, $y \in B$ and $y \in C$ and so $y \in B \cap C$. We conclude that $p = (x, y) \in A \times (B \cap C)$ and so $(A \times B) \cap (A \times C) \subseteq A \times (B \cap C)$.

   Remark: from now on, we will immediately refer to an element of a Cartesian product as an ordered pair, rather than deriving it as part of the proof.

4. Assume that there exists a $(x, y) \in (A \times B) \cup (C \times D)$. Then, $(x, y) \in A \times B$ or $(x, y) \in C \times D$. There are two cases:

   (a) *Case 1 –* $(x, y) \in A \times B$*:* this implies that $x \in A$ and $y \in B$, and so $x \in A \cup C$ and $y \in B \cup D$, implying that $(x, y) \in (A \cup C) \times (B \cup D)$.

   (b) *Case 2 –* $(x, y) \in C \times D$*:* this implies that $x \in C$ and $y \in D$, and so $x \in A \cup C$ and $y \in B \cup D$, implying that $(x, y) \in (A \cup C) \times (B \cup D)$.

   Since (x, y) is any element, we have that $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$.

5. Assume that $A \times \emptyset \neq \emptyset$. Then it has an element (x, y) implying that $y \in \emptyset$, which is a contradiction. The proof that $\emptyset \times A = \emptyset$ is similar (*you are not allowed to say this in your proofs*!).

■

A shorter proof of the first item of Theorem 4.3 is as follows:

$$\begin{aligned}(x,y) \in A \times (B \cap C) &\Leftrightarrow x \in A \wedge y \in B \cap C \\ &\Leftrightarrow x \in A \wedge y \in B \wedge y \in C \\ &\Leftrightarrow x \in A \wedge y \in B \wedge x \in A \wedge y \in C \\ &\Leftrightarrow (x,y) \in A \times B \wedge (x,y) \in A \times C \\ &\Leftrightarrow (x,y) \in (A \times B) \cap (A \times C)\end{aligned}$$

Item (4) of Theorem 4.3 does not state equivalence. In an attempt to understand what happens in the reverse direction, let us start with some $(x,y) \in (A \cup C) \times (B \cup D)$. This implies that $x \in A \cup C$ and $y \in B \cup D$. Thus, $x \in A$ or $x \in C$ and $y \in B$ or $y \in D$. It is very possible that $x \in A$ and $y \in D$ in which case $(x,y) \notin A \times B$ or $C \times D$. Given this analysis, we can come up with a concrete counterexample. Specifically, let $A = \{a\}$, $D = \{d\}$ and let $B = C = \emptyset$. It follows that $(A \cup C) \times (B \cup D) = \{(a,d)\}$. However, $A \times B = \emptyset$ and $C \times D = \emptyset$ (by applying item (5)), and thus $(A \times B) \cup (C \times D) \neq (A \cup C) \times (B \cup D)$. This is an example of a case where it sometimes helps to try to prove a incorrect statement in order to find a counterexample.

Example 4.4 *Prove or disprove: Let A and B be sets. Then, $A \times B = B \times A$ if and only if $A = B$.*

Proof: We begin by proving that if $A \times B = B \times A$ then $A = B$. Let $x \in A$ and let $y \in B$. Then, $(x,y) \in A \times B = B \times A$. This implies that $x \in B$ and $y \in A$. Since x is an arbitrary element of A we have that $A \subseteq B$, and since y is an arbitrary element of B we have that $B \subseteq A$. Thus, $A = B$.

For the other direction, if $A = B$ then syntactically $A \times B$ is the same as $B \times A$. ■

Disproof: Let A be any set (e.g., $A = \{1,2,3\}$) and let $B = \emptyset$. Then, by Theorem 4.3 we have that $A \times B = B \times A = \emptyset$. But, $A \neq B$. ■

How do we have a counterexample and a proof at the same time? The answer is that we don't; the proof is incorrect. This is an excellent example of why one must be very careful not to assume *anything* when writing a proof. Specifically, our "proof" began with the statement: let $x \in A$ and let $y \in B$. This is an assumption that neither A nor B are empty. The counterexample holds exactly where this omission lies. Observe that when we wish to prove $A \subseteq B$ then we typically begin with "assume that $x \in A$" and then proceed. This is fine since a proof that $A \subseteq B$ is a proof that "$x \in A \Rightarrow x \in B$" and so we only need to prove the statement for values x for which $x \in A$. In contrast, in the proof above, we can only assume that $A \times B = B \times A$ and cannot assume that there is any element in this set.

This discussion leads us to the correct version of this theorem:

Theorem 4.5 *Let A and B be sets. Then, $A \times B = B \times A$ if and only if either $A = \emptyset$, $B = \emptyset$ or $A = B$.*

We leave the proof of this theorem for an exercise; after what we have seen above it is not difficult.

Extensions: It is possible to define an n-tuple $(a_1, \ldots, a_n)$ as an ordered vector, based on an order pair, as follows:

$$(a_1, \ldots, a_n) = \begin{cases} (a_1, (a_2, \ldots, a_n)) & n > 2 \\ (a_1, a_n) & n = 2 \end{cases}$$

The cartesian product of n sets is defined in the natural way using the notion of an n-tuple.

4.2 Relations Basics

Definition 4.6 *Let A and B be sets. A set $R \subseteq A \times B$ is called a* binary relation*, and is also called a* relation from A to B*. For $(a, b) \in R$, we denote $R(a, b)$ or aRb, and for $(a, b) \notin R$ we denote $\neg R(a, b)$ or $\neg aRb$. If $R \subseteq A \times A$ then we say that R is a* relation on A*.*

1. The relation $\{(a, b) \mid a, b \in \mathbb{N} \wedge \exists c \in \mathbb{N} \setminus \{0\}(b = a + c)\}$ is called the "less than" relation.
2. $A = \{1, \ldots, 10\}$, $B = \{1, \ldots, 4\}$, $R = \{(1, 1), (2, 4), (4, 2)\}$ is a relation
3. $\{(m, n) \mid m, n \in \mathbb{N} \wedge m|n\}$
4. $\{(m, m) \mid m \in \mathbb{R}\}$ is the "equals" relation

Definition 4.7 *Let R be a relation from A to B. Then, the* domain *of R is the set*

$$\mathrm{Dom}(R) = \{a \in A \mid \exists b \in B((a, b) \in R)\}$$

and the range *is the set*

$$\mathrm{Ran}(R) = \{b \in B \mid \exists a \in A((a, b) \in R)\}.$$

The inverse *of R is the relation R^{-1} from B to A is defined as*

$$R^{-1} = \{(b, a) \in B \times A \mid (a, b) \in R\}.$$

Let R be a relation from A to B and S a relation from B to C. The composition *of S and R, denoted $S \circ R$, is a relation from A to C defined by*

$$S \circ R = \{(a, c) \in A \times C \mid \exists b \in B((a, b) \in R \wedge (b, c) \in S\}$$

Note that the composition of S and R is only defined if R is defined *to* a set B, and S is defined *from* that same set B. Observe that we write $S \circ R$ even though R "comes first". The reason for this notation is that if you view a relation as a *mapping* from the first set to the second, then you first apply the mapping of R to some a and then the mapping of S to the result. This notation will make more sense when we study functions.

Example 4.8 *Prove or disprove: Let R be a relation from A to B and let S be a relation from B to C. Then, $S \circ R = \emptyset$ if and only if $A = \emptyset$ or $B = \emptyset$ or $C = \emptyset$ or $S = \emptyset$ or $R = \emptyset$.*

We provide a counterexample: consider $A = B = C = \mathbb{N}$; $R = S = \{(1, 2)\}$. In general, when searching for counterexample, try to find simple and concise counterexamples.

Theorem 4.9 *Let R be a relation from A to B, S be a relation from B to C, and T be a relation from C to D. Then:*

1. $(R^{-1})^{-1} = R$
2. $\mathrm{Dom}(R^{-1}) = \mathrm{Ran}(R)$
3. $\mathrm{Ran}(R^{-1}) = \mathrm{Dom}(R)$
4. $T \circ (S \circ R) = (T \circ S) \circ R$
5. $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$

Proof:

1. First, by definition, R^{-1} is a relation from B to A and thus $(R^{-1})^{-1}$ is a relation from A to B. Now, $(a, b) \in (R^{-1})^{-1}$ iff $(b, a) \in R^{-1}$ iff $(a, b) \in R$.

2. First, $\text{Ran}(R) \subseteq B$ and $\text{Dom}(R^{-1}) \subseteq B$. Next, let b be an arbitrary element. Then,

$$b \in \text{Dom}(R^{-1}) \;\Leftrightarrow\; \exists a \in A \left((b,a) \in R^{-1}\right) \;\Leftrightarrow\; \exists a \in A \left((a,b) \in R\right) \;\Leftrightarrow\; b \in \text{Ran}(R).$$

3. By item (2) we have $\text{Ran}(R^{-1}) = \text{Dom}((R^{-1})^{-1})$ and by item (1) we have that $(R^{-1})^{-1} = R$. Thus, $\text{Ran}(R^{-1}) = \text{Dom}(R)$.

   Remark: This proof illustrates an important methodology in mathematics. It is better to prove a theorem or claim by relying on previously proven claims, when possible, than by proving it from scratch.

We leave the last two for an exercise. ∎

We are often interested in relations that connect two items of the same type; i.e., relations $R \subseteq A \times A$. In such a case, we say that R is a *relation on the set* A.

Definition 4.10 *Let A be a set, and let R be a relation on A.*

- *R is called* reflexive *if for every $x \in A$ it holds that $(x,x) \in R$*
- *R is called* symmetric *if for every $x, y \in A$ it holds that $(x,y) \in R \;\Leftrightarrow (y,x) \in R$*
- *R is called* transitive *if for every $x, y, z \in A$ it holds that $(x,y) \in R \;\wedge\; (y,z) \in R \;\Rightarrow\; (x,z) \in R$*

Example 4.11 *1. Define the identity relation i_A on a set A by $\{(x,x) \mid x \in A\}$. Then, i_A is reflexive, symmetric and transitive.*

2. The empty set ϕ is a relation by definition. Furthermore, it is always symmetric and transitive. If we consider ϕ as a relation over A, then ϕ is reflexive if and only if $A = \phi$.

Theorem 4.12 *Let R be a relation on A. Then,*

1. *R is reflexive if and only if $i_A \subseteq R$, where i_A is the identity relation.*
2. *R is symmetric if and only if $R = R^{-1}$.*
3. *R is transitive if and only if $R \circ R \subseteq R$.*

Proof: We prove the second item, and we assume that $R \neq \emptyset$ (otherwise, it is trivial). Assume that R is symmetric, and let $(x,y) \in R$ and so xRy. Since R is symmetric we have that yRx and thus $(y,x) \in R$. By the definition of R^{-1} we have that $(x,y) \in R^{-1}$. This implies that $R \subseteq R^{-1}$. Likewise, for any $(x,y) \in R^{-1}$ we have that $(y,x) \in R$ and then by the fact that R is symmetric $(x,y) \in R$. Thus, $R^{-1} \subseteq R$ and we conclude that $R = R^{-1}$.

Next, assume that $R = R^{-1}$. We have:

$$(x,y) \in R \quad \Leftrightarrow \quad (y,x) \in R^{-1} \quad \Leftrightarrow \quad (y,x) \in R$$

where the first "$\Leftrightarrow$" is by the definition of R^{-1} and the second "$\Leftrightarrow$" is due to the fact that $R = R^{-1}$. We therefore have that R is symmetric. ∎

4.3 Ordering Relations

Observe that the $\leq$ relation is reflexive and transitive, but is *not* symmetric in a very strong way. Specifically, symmetry only holds for elements that are the same (i.e., $x \leq y$ and $y \leq x$ if and only if $x = y$).

Definition 4.13 *Let R be a relation on a set A. Then, R is* antisymmetric *if for every $x, y \in A$, if xRy and yRx then $x = y$.*

Example 4.14 *Let A be a set, and let $B = \mathcal{P}(A)$. Define $R = \{(X, Y) \in B \times B \mid X \subseteq Y\}$. Then, R is reflexive, transitive, and antisymmetric. Likewise, consider the "divisible" relation.*

Both the $\leq$ relation, and R in the previous example, actually define an ordering on the sets (they compare "sizes" in an intuitive sense). The reason for this is that we can place elements in order x, y, z by xRy and yRz (where by transitivity we know that xRz as well). This is not enough since it may also hold that zRx and so we have a "cycle" and no ordering. However, this would then contradict antisymmetry. Thus, the combination of the above provides an ordering (sometimes reflexivity is replaced with irreflexivity in the case of a strict ordering, as in the $<$ relation).

However, there is a difference in that for all numbers x and y it holds that either $x \leq y$ or $y \leq x$, but there exist sets $X, Y \in B$ such that $X \not\subseteq Y$ and $Y \not\subseteq X$.

Definition 4.15 *Let R be a relation on a set A. Then, R is a* partial order *on A if it is reflexive, transitive and antisymmetric. It is called a* total order *on A if it is a partial order, and in addition for every $x, y \in A$ it holds that either xRy or yRx.*

Based on the above, the $\leq$ relation is a total order, and the relation R in Example 4.14 is a partial order but not a total order.

Once we consider ordering, we can talk about a smallest or largest element in the set. However, in the case of a partial order, it is possible that there are two elements that are "smallest".

Definition 4.16 *Let R be a partial order on a set A, let $B \subseteq A$, and let $b \in B$. Then, b is an R-*smallest element of *B if for every $x \in B$ it holds that bRx. The value b is called an R-*minimal *element if there exists no $x \in B$ with $x \neq b$ such that xRb.*

Observe that a minimal element is one that has no element smaller than it, whereas a smallest element is smaller than all other elements in B. Considering Example 4.14, $\emptyset$ is a smallest element. However, if we redefine B to be $\mathcal{P}(A) \setminus \emptyset$, then all singletons are minimal elements.

Theorem 4.17 *Let R be a partial order on a set A and let $B \subseteq A$.*

1. *If B has a smallest element, then it is unique (thus it is* the *smallest element).*
2. *Assume that b is the smallest element of B. Then, b is also a minimal element of B, and is the only minimal element.*
3. *If R is a total order and b is a minimal element of B, then b is the smallest element of B.*

Proof:

1. Assume that b and c are smallest elements of B. Since b is a smallest element, it holds that $\forall x \in B(bRx)$ and in particular bRc. Likewise, since c is a smallest element $\forall x \in B(cRx)$ and in particular cRb. Since R is a partial order it is antisymmetric and thus from bRc and cRb we have that $b = c$, as required.
2. Assume that b is the smallest element of B. We begin by showing that b is a minimal element. Our proof works by showing that $\forall x \in B(xRb \Rightarrow x = b)$.[2] Let $x \in B$ and assume that xRb. Since b is the smallest element of B it holds that bRx. Thus, by antisymmetry we have that $x = b$.

   Next we prove that b is the only minimal element. Let c be a minimal element. Since b is the smallest element, we have that bRc. However, since c is minimal, we have that there does not exist any $x \in B$ such that $x \neq c$ and xRc. Since bRc and $b \in B$ it must be that $c = b$.

[2] We need to prove $\neg\exists x \in B(xRb \wedge x \neq b)$ which is logically equivalent to $\neg\exists x \in B\neg(\neg xRb \vee x = b)$ which is turn logically equivalent to $\forall x \in B(xRb \Rightarrow x = b)$.

3. Let R be a total order and b a minimal element of B. We show that $\forall x \in B(bRx)$. Let $x \in B$. If $x = b$ then bRx by reflexivity. Else, $x \neq b$. Since R is a total order, we have that either xRb or bRx. However, xRb cannot be true since b is minimal (and $x \neq b$). Thus, bRx and so b is the smallest element of B.

■

Not all sets have a minimum, even they are bounded. For example, consider $\mathbb{Q}$ and the subset $I = \{\frac{1}{n}\}_{n\in\mathbb{N}}$, and the $\leq$ relation. Then, $I \subseteq \mathbb{Q}$ is bounded since all values are between 0 and 1. However, I has no minimal or smallest element; for every $x \in I$ we have that $x = \frac{1}{\ell}$ for some ℓ and then $\frac{1}{\ell+1} \in I$ and $\frac{1}{\ell+1} < \frac{1}{\ell}$. This yields the following definition:

Definition 4.18 *Let R be a partial order on A, let $B \subseteq A$ and let $a \in A$. Then, a is called a* lower bound *for B if for every $x \in B$ it holds that aRx. Similarly, a is an* upper bound *for B if $\forall x \in B(xRa)$.*

Observe that 0 is a *lower bound* for the set I defined above, but it is not a member of I.

Definition 4.19 *Let R be a partial order on A and let $B \subseteq A$. Let U be the set of all upper bounds for B, and let L be the set of all lower bounds. If U has a smallest element, then this smallest element is called the* least upper bound *(l.u.b.) of B. If L has a largest element, then this largest element is called the* greatest lower bound *(g.l.b.) of B.*

For every positive number $x > 0$, there exists an n such that $\frac{1}{n} < x$. Thus, the set L of all lower bounds of I defined above is $L = \{x \in \mathbb{R} \mid x \leq 0\}$. Since L has a largest element, the number 0, it follows that I has a greatest lower bound. Note that 1 is the largest element of I and that this is also an upper bound, and the least upper bound.

Theorem 4.20 *Let A be a set, and let $F \subseteq \mathcal{P}(A)$ with $F \neq \emptyset$. Let $R = \{(X, Y) \in F \times F \mid X \subseteq Y\}$. Then, the least upper bound of F is $\cup F$ and the greatest lower bound of F is $\cap F$.*

Proof: Define $U = \{Y \subseteq A \mid \forall X \in F(X \subseteq Y)\}$ to be the set of all upper bounds. Clearly, $\cup F \in U$ since $\cup F \subseteq A$ and by definition of $\cup F$ it holds that $\forall X \in F(X \subseteq \cup F)$. Next, we claim that $\cup F$ is the smallest element of U. In order to see this, let $Y \in U$. By the definition of U, it holds that $\forall X \in F(X \subseteq Y)$. Now, let $x \in \cup F$. Then, there exists a set $X \in F$ such that $x \in X$. Since $\forall X \in F(X \subseteq Y)$ we have that $x \in Y$. Thus, $\cup F \subseteq Y$. This implies that $\cup F$ is the smallest element of U and so is the least upper bound of F.

We leave the proof that $\cap F$ is the greatest lower bound as an exercise. ■

4.4 Closures

The only difference between the $<$ and $\leq$ relations is that the latter also contains elements that are equal. Thus, one can view $\leq$ as being obtained from $<$ by adding all pairs (x, x). In fact, $\leq$ is the *smallest* set that is obtained from $<$ and is reflexive. Observe that by "smallest" here, we mean in the formal sense, based on the subset relation defined previously.

Definition 4.21 *Let R be a relation on a set A. Then, $S \subseteq A \times A$ is the reflexive closure of R if it has the following three properties:*

1. *$R \subseteq S$*
2. *S is reflexive*
3. *For every relation $T \subseteq A \times A$, if $R \subseteq T$ and T is reflexive, then $S \subseteq T$.*

Another way of stating Definition 4.21 is that the reflexive closure of R is the smallest set $S \subseteq A \times A$ such that $R \subseteq S$ and S is reflexive (if there is such a smallest set). As we have seen, not all sets have a smallest element. Thus, we need to prove that every relation has a reflexive closure.

Theorem 4.22 *Let R be a relation on a set A. Then, R has a reflexive closure.*

Proof: Let $S = R \cup i_A$, where i_A is the identity relation on A (i.e., $i_A = \{(a, a) \mid a \in A\}$). We claim that S is the reflexive closure of R. Clearly, $R \subseteq S$. In addition, S is reflexive since $i_A \subseteq S$ and this implies reflexivity by Theorem 4.12. Finally, assume that $T \subseteq A \times A$, $R \subseteq T$ and T is reflexive. Since T is reflexive we have that $i_A \subseteq T$ (again by Theorem 4.12). Since we also have that $R \subseteq T$ we can conclude that $S = R \cup i_A \subseteq T$. ∎

Not all orders are reflexive, as we have seen with the $<$ relation.

Definition 4.23 *Let R be a relation on A. Then, R is* irreflexive *if $\forall x \in A((x, x) \notin R)$. R is a* strict partial order *if it is irreflexive and transitive. R is a* strict total order *if it is a strict partial order and for every $x, y \in A$ either xRy or yRx or $x = y$ (this property is called* trichotomy*).*

We stress that a strict partial order is *not* a partial order. In addition, observe that antisymmetry is not required in Definition 4.23. This is because if xRy and yRx then xRx by transitivity, which contradicts irreflexibility. Thus, for no two elements does it hold that xRy and yRx.

We can define symmetric and transitive closures in the same way.

Definition 4.24 *Let R be a relation on A. A relation $S \subseteq A \times A$ is the* symmetric closure *of R if it has the following three properties:*

1. *$R \subseteq S$*
2. *S is symmetric*
3. *For every relation $T \subseteq A \times A$, if $R \subseteq T$ and T is symmetric, then $S \subseteq T$.*

A relation $S \subseteq A \times A$ is the transitive closure *of R if it has the following three properties:*

1. *$R \subseteq S$*
2. *S is transitive*
3. *For every relation $T \subseteq A \times A$, if $R \subseteq T$ and T is transitive, then $S \subseteq T$.*

Theorem 4.25 *Let R be a relation on a set A. Then, R has a symmetric closure.*

Proof: Let $S = R \cup R^{-1}$. It is immediate that $R \subseteq S$. In addition, $S^{-1} = R^{-1} \cup R = R \cup R^{-1} = S$ and thus by Theorem 4.12 S is symmetric. Finally, let $T \subseteq A \times A$ such that $R \subseteq T$ and T is symmetric. We show that $S \subseteq T$. Let $(x, y) \in S$. If $(x, y) \in R$ then since $R \subseteq T$ we have that $(x, y) \in T$. If $(x, y) \in R^{-1}$ then $(y, x) \in R$ and so $(y, x) \in T$. However, since T is symmetric, this implies that $(x, y) \in T$ as well. Thus, $S \subseteq T$. ∎

Theorem 4.26 *Let R be a relation on a set A. Then, R has a transitive closure.*

Proof: Let $F = \{T \subseteq A \times A \mid R \subseteq T \text{ and } T \text{ is transitive}\}$; i.e., F is the set of all transitive relations containing R. Now, since $R \subseteq A \times A$ and $A \times A$ is transitive, we have that $A \times A \in F$ and so $F \neq \emptyset$. Thus, we can define $S = \cap F$. We will prove that S is the transitive closure of R. We prove each of the three properties:

1. Let $(x, y) \in R$, and let $T \in F$. Then, since $R \subseteq T$ we have that $(x, y) \in T$. Thus, $\forall T \in F((x, y) \in T)$ and so $(x, y) \in \cap F = S$.
2. Let $(x, y) \in S$, let $(y, z) \in S$, and let $T \in F$. Since $(x, y) \in S = \cap F \subseteq T$ and $(y, z) \in S = \cap F \subseteq T$ we have that $(x, y) \in T$ and $(y, z) \in T$. Now, by the definition of F, the relation T is transitive and thus $(x, z) \in T$. Thus, $\forall T \in F((x, z) \in T)$, and thus $(x, z) \in \cap F = S$.
3. Let $T \subseteq A \times A$, $R \subseteq T$ such that T is transitive. By the definition of F, $T \in F$. Since $S = \cap F$ it follows immediately that $S \subseteq T$.

∎

4.5 Equivalence Relations

An *equivalence relation* is a relation that expresses equality. In terms of the properties of relations that we have seen so far, equality should be *reflexive* (since $x = x$ always), *symmetric* (since if $x = y$ then $y = x$), and *transitive* (since if $x = y$ and $y = z$ then $x = z$). This yields the following definition:

Definition 4.27 *Let R be a relation on a set A. Then, R is an* equivalence relation *on A if it is reflexive, symmetric and transitive.*

Example 4.28 *Consider the relation of "congruence mod n", defined on $\mathbb{Z}$ as follows: $x \equiv y \bmod n$ if x and y have the same remainder when divided by n (equivalently, if $n \mid (x - y)$). We claim that this relation is an equivalence relation. In order to see this, observe that it is trivially reflexive and symmetric. Regarding transitivity, assume that $x \equiv y \bmod n$ and $y \equiv z \bmod n$. Write $x = q \cdot n + r$. Then, since $x \equiv y \bmod n$ we have that $y = q' \cdot n + r$ (i.e., it has the same remainder). Likewise, since $y \equiv z \bmod n$ we have that $z = q'' \cdot n + r$. Thus, x and z have the same remainder when divided by n.*

It is important to note that congruence mod n is not at all the same as equality of numbers. For example, taking $n = 7$, we have that $1 \equiv 8$ and $1 \equiv 15 \bmod 7$. Nevertheless, within the context of mod 7 *they are the same.*

Definition 4.29 *Let R be an equivalence relation on A and let $x \in A$. Then, the* equivalence class *of x with respect to R is the set $[x]_R = \{y \in A \mid yRx\}$.*

The set of all equivalence classes of elements of A is called A modulo R and is denoted A/R. Formally,

$$A/R = \{[x]_R \mid x \in A\} = \{X \subseteq A \mid \exists x \in A(X = [x]_R)\}.$$

Where it is clear from the context, we use the notation $[x]$ instead of $[x]_R$.

Example 4.30 *Continuing the previous example with $n = 7$, we have that $[1] = \{1, 8, 15, 22, 29, ...\}$. More formally, $[0] = \{7i \mid i \in \mathbb{Z}\}$, $[1] = \{1 + 7i \mid i \in \mathbb{Z}\}$, $[2] = \{2 + 7i \mid i \in \mathbb{Z}\}$, and so on. In addition, $\mathbb{Z}/R = \{[0], [1], [2], [3], [4], [5], [6]\}$, where R is congruence* mod 7.

We now prove a helpful lemma.

Lemma 4.31 *Let R be an equivalence relation on A. Then, for every $x \in A$, $x \in [x]$. Furthermore, for every $x, y \in A$ we have that $y \in [x]$ if and only if $[y] = [x]$.*

Proof: Let $x \in A$. Since R is reflexive xRx and thus $x \in [x]$.

Regarding the "furthermore" part, let $x, y \in A$. Assume first that $y \in [x]$. This implies that yRx. Now, let $z \in [y]$; this implies that zRy and by transitivity that zRx and thus $z \in [x]$. Thus $[y] \subseteq [x]$. Next, let $z \in [x]$ and so zRx. We already have that yRx and so by symmetry we have that xRy. Thus, by transitivity we have that zRy implying that $z \in [y]$. Thus $[x] \subseteq [y]$ and so $[x] = [y]$.

Next, assume that $[y] = [x]$. From the first claim in the theorem we know that $y \in [y]$. But since $[y] = [x]$ we have that $y \in [x]$, as required. ∎

Theorem 4.32 *Let R be an equivalence relation on A. Then A/R is a partition of A.*

Proof: We begin by proving that $\cup(A/R) = A$, or stated differently that $\cup_{x \in A}[x] = A$. For every equivalence class $[x] \in A/R$ it holds that $[x] \subseteq A$. Thus, $\cup_{x \in A}[x] \subseteq A$ (the proof that the union of a family of subsets of A is a subset of A, is left for an exercise). Next, let $x \in A$. Then, by Lemma 4.31 it follows that $x \in [x]$. In addition, $[x] \in A/R$ and thus $x \in \cup(A/R)$. Therefore, $\cup(A/R) = A$.

Next, we prove that A/R is pairwise disjoint. Let $X, Y \in A/R$; by the definition of A/R there exist $x, y \in A$ such that $X = [x]$ and $Y = [y]$. If $X \cap Y \neq \emptyset$, then there exists a $z \in X \cap Y = [x] \cap [y]$. By Lemma 4.31 it follows that $[x] = [z]$ and $[y] = [z]$ and thus $[x] = [y]$, or equivalently $X = Y$. This implies that the elements of A/R are all pairwise disjoint (for every X, Y such that $X \neq Y$ we have that $X \cap Y = \emptyset$).

Finally, we show that $\emptyset \notin A/R$. Let $X \in A/R$; by the definition of A/R there exists an $x \in A$ such that $X = [x]$. Then, by Lemma 4.31 we have that $x \in [x] = X$ and so $X \notin \emptyset$. ∎

In the above, we have shown that every equivalence relation defines a partition of A. We will now show the converse which is that every partition defines an equivalence relation.

Theorem 4.33 *Let A be a set and let $\mathcal{F}$ be a partition of A. Then, there exists an equivalence relation R on A such that $A/R = \mathcal{F}$.*

Proof: We prove the theorem by finding an actual equivalence relation, based on the structure of $\mathcal{F}$. We will do this by considering the relation made up of all pairs of elements in the same set of the partition. That is, if x and y are in the same set in the partition of $\mathcal{F}$, then we will define xRy. This will ensure equivalence. We begin by proving two lemmas.

Lemma 4.34 *Let A be a set and let $\mathcal{F}$ be a partition of A. Let $R = \cup_{X \in \mathcal{F}}(X \times X)$. Then, R is an equivalence relation on A, and is called* the equivalence relation determined by $\mathcal{F}$.

Proof: We need to prove reflexivity, symmetry and transitivity. Let $x \in A$. Since $\mathcal{F}$ is a partition of A, there exists a set $X \in \mathcal{F}$ such that $x \in X$. Thus, $(x, x) \in X \times X$ and so xRx. Regarding symmetry: let $x, y \in A$ such that xRy (if no such x, y exist then symmetry holds trivially). This implies that $(x, y) \in X \times X$ for some $X \in \mathcal{F}$, and thus that $x, y \in X$. However, this implies that $(y, x) \in X \times X$ as well, and so yRx, as required. We leave the proof of transitivity as an exercise. ∎

Lemma 4.35 *Let A be a set, let $\mathcal{F}$ be a partition of A, and let R be the equivalence relation determined by $\mathcal{F}$. If $X \in \mathcal{F}$ and $x \in X$, then $[x] = X$.*

Proof: Assume that $X \in \mathcal{F}$ and $x \in X$. In order to prove that $X = [x]$, we prove that $y \in [x] \Leftrightarrow y \in X$. Let $y \in [x]$ and so $(y, x) \in R$. By the definition of R this implies that there exists a set $Y \in \mathcal{F}$ such that $(x, y) \in Y \times Y$, and so $x \in Y$ and $y \in Y$. We have that $x \in X$ and $x \in Y$ and thus $X \cap Y \neq \emptyset$. However, $\mathcal{F}$ is pairwise disjoint and thus $X = Y$. We conclude that $y \in X$ and so $[x] \subseteq X$.

Next, assume that $y \in X$. Then, $(y, x) \in X \times X$ and so $(y, x) \in R$ (because by the assumption $x \in X$). This implies that $y \in [x]$ and thus $X \subseteq [x]$, completing the proof that $[x] = X$. ∎

We are now ready to complete the proof of Theorem 4.33. Let $R = \cup_{X \in \mathcal{F}}(X \times X)$. We have already proven that R is an equivalence relation and so it remains to prove that $A/R = \mathcal{F}$. Let $X \in A/R$. Then, $X = [x]$ for some $x \in A$. Since $\mathcal{F}$ is a partition we have that $\cup\mathcal{F} = A$ and so $x \in \cup\mathcal{F}$. Thus, there exists a set $Y \in \mathcal{F}$ such that $x \in Y$. By Lemma 4.35, $[x] = Y$ and thus $X = Y$, implying that $X \in \mathcal{F}$. We therefore have that $A/R \subseteq \mathcal{F}$.

Next, let $X \in \mathcal{F}$. Since $\mathcal{F}$ is a partition, $X \neq \emptyset$ and so there exists an element $x \in X$. By Lemma 4.35, $X = [x]$ and $[x] \in A/R$. Thus, $X \in A/R$ and so $\mathcal{F} \subseteq A/R$, implying that $A/R = \mathcal{F}$. ∎

Example 4.36 *Let P be the set of all computer programs, and define the relation R so that $(p, q) \in R$ if p and q always produce the same output (or do not halt at all) upon the same input. It is not hard to see that R is an equivalence relation. An interesting question is whether or not one can write a computer program that will determine for any two programs p and q if pRq or $\neg(pRq)$.*

5 Functions

A function is just a special type of relation with the property that for every x there exists a *single* y such that $(x, y) \in R$. Functions are typically denoted by $y = f(x)$ since $f(x)$ defines a single value. Of course, it is possible that there be many values of x for which $y = f(x)$, but for every x there can be just one y.

Definition 5.1 *Let F be a relation from A to B. Then, F is a* function from A to B *if for every $a \in A$ there exists exactly one $b \in B$ such that $(a, b) \in F$. That is:*

$$\forall a \in A \exists! b \in B((a, b) \in F)$$

In this case, we write $F : A \to B$, and we denote $b = F(a)$.

Observe that f must be defined for *every* $a \in A$. Thus, the domain of f is always all of A (in contrast to the way relations are defined which can be over a subset of A).

Theorem 5.2 *Let f and g be functions from A to B. If $\forall a \in A(f(a) = g(a))$ then $f = g$.*

Proof: Assume that $\forall a \in A(f(a) = g(a))$. Let $(a, b) \in f$ and so $b = f(a)$. By the assumption, $b = g(a)$ and so $(a, b) \in g$ as well. Thus $f \subseteq g$. The opposite direction is similar. Thus, $f = g$. ∎

We have already defined the domain and range of a relation, and this is the same. However, in the context of functions the result is a bit different. First, as we have seen, $\text{Dom}(f) = A$ always. Next, the range of a function can equivalently be defined by:

$$\text{Ran}(f) = \{f(a) \mid a \in A\}.$$

Theorem 5.3 *Let $f : A \to B$ and $g : B \to C$. Then, $g \circ f : A \to C$ is a function, and for any $a \in A$ it holds that $g \circ f(a) = g(f(a))$.*

Proof: Let $a \in A$ be an arbitrary element. In order to prove the above, we have to show that there exists a unique element $c \in C$ such that $g \circ f(a) = c$ (this proves that $g \circ f$ is a function), and we have to show that $g \circ f(a) = g(f(a))$ for all $a \in A$.

We begin by showing *existence*. Let $b = f(a) \in B$, and let $c = g(b) \in C$ (observe that these are defined since the respective domains of f and g are all of A and B). This implies that $(a, b) \in f$ and $(b, c) \in g$ and so by the definition of composition of relations we have that $(a, c) \in g \circ f$.

We next show *uniqueness*. Assume that there exist $c_1, c_2 \in C$ such that $(a, c_1) \in g \circ f$ and $(a, c_2 \in g \circ f$. By the definition of composition, this implies that there exist $b_1, b_2 \in B$ such that $(a, b_1) \in f$, $(b_1, c_1) \in g$, $(a, b_2) \in f$ and $(b_2, c_2) \in g$. Since f is a function, there exists a single b such that $(a, b) \in f$. Thus, $b_1 = b_2$. Likewise, since g is a function, there exists a single c such that $(b_1, c) = (b_2, c) \in g$. Thus, $c_1 = c_2$, as required.

It remains to show that the formula for computing $g \circ f(a)$ is $g(f(a))$. This follows from the existence proof where we showed that if we take $b = f(a)$ and $c = g(b)$ then we obtain that $(a, c) \in g \circ f$. ∎

The above theorem explains the strange notation of $g \circ f$ for composition of relations. Specifically, we write $g \circ f$ and not $f \circ g$ because of the formula $g(f(x))$.

Inverses. Recall that for any relation R^{-1} defines its inverse. Furthermore, its inverse always exists. In the case of functions, the inverse is not necessarily a function. This is because the range of $f : A \to B$ may not be the entire set B in which case f is not a function from B to A. Furthermore, if there exists a_1, a_2, b such that $f(a_1) = f(a_2) = b$ then $f^{-1}(b)$ does not define a single value. We now define what is required of f so that its inverse is a function.

Definition 5.4 *Let $f : A \to B$ be a function. f is* one-to-one*, and called an* injection*, if*

$$\neg(\exists a_1 \in A \exists a_2 \in A(f(a_1) = f(a_2) \wedge a_1 \neq a_2))$$

f is onto*, and called a* surjection*, if*

$$\forall b \in B \exists a \in A(f(a) = b)$$

A function that is both one-to-one and onto is called a bijection*.*

We now prove a theorem that makes it easy to determine whether a function is one-to-one or onto.

Theorem 5.5 *Let $f : A \to B$ be a function. Then, f is one-to-one if and only if*

$$\forall a_1 \in A \forall a_2 \in A(f(a_1) = f(a_2) \Rightarrow a_1 = a_2,$$

and f is onto if and only if $\text{Ran}(f) = B$*.*

Proof: We prove the first part of the theorem by applying the equivalence rules from logic. A function f is one-to-one if and only if

$$\begin{aligned} \neg(\exists a_1 \in A \exists a_2 \in A(f(a_1) = f(a_2) \wedge a_1 \neq a_2)) &\Leftrightarrow \forall a_1 \in A \forall a_2 \in A \neg(f(a_1) = f(a_2) \wedge a_1 \neq a_2) \\ &\Leftrightarrow \forall a_1 \in A \forall a_2 \in A(f(a_1) \neq f(a_2) \vee a_1 = a_2) \\ &\Leftrightarrow \forall a_1 \in A \forall a_2 \in A(f(a_1) = f(a_2) \Rightarrow a_1 = a_2). \end{aligned}$$

We now proceed to part 2 of the theorem. f is onto if and only if $\forall b \in B \exists a \in A(f(a) = b)$, which is equivalent to saying that $\forall b \in B \exists a \in A((a, b) \in f)$. By the definition of the range, this is equivalent to saying that $\forall b \in B(b \in \text{Ran}(f))$ and thus $B \subseteq \text{Ran}(f)$. This proves that f is onto if and only if $B \subseteq \text{Ran}(f)$.

Now, if f is onto then we already have proven that $B \subseteq \text{Ran}(f)$. However, by the definition of range, it always holds that $\text{Ran}(f) \subseteq B$. Thus, $\text{Ran}(f) = B$. For the other direction, assume that $\text{Ran}(f) = B$. Then, it immediately follows that $B \subseteq \text{Ran}(f)$ and by what we have already shown this proves that f is onto. ∎

Example 5.6 *Let $A = \mathbb{R} \setminus \{-1\}$, and define $f : A \to \mathbb{R}$ by $f(a) = \frac{2a}{a+1}$. Prove that f is one-to-one by not onto.*

Proof: We prove that f is one-to-one using Theorem 5.5. Let $a_1, a_2 \in A$ and assume that $f(a_1) = f(a_2)$. Then, $\frac{2a_1}{a_1+1} = \frac{2a_2}{a_2+1}$, implying that $2a_1(a_2+1) = 2a_2(a_1+1)$ and so $2a_1a_2 + 2a_1 = 2a_2a_1 + 2a_2$. We conclude that $2a_1 = 2a_2$ and so $a_1 = a_2$.

In order to prove that f is not onto, we show that $2 \notin \text{Ran}(f)$. Assume by contradiction that there exists $a \in A$ such that $f(a) = 2$. This implies that $\frac{2a}{a+1} = 2$ and so $\frac{a}{a+1} = 1$, implying that $a = a + 1$, which is impossible. ∎

We now prove a theorem regarding when f has an inverse.

Theorem 5.7 *Let $f : A \to B$ be a function. If f is one-to-one and onto, then f has an inverse function ($f^{-1} : B \to A$).*

Proof: Assume that f is one-to-one and onto, and let $b \in B$ be an arbitrary element. We prove that there exists a unique $a \in A$ such that $(b, a) \in f^{-1}$. Regarding existence: since f is onto there exists some $a \in A$ such that $f(a) = b$ and so $(b, a) \in f^{-1}$. Regarding uniqueness: let $a_1, a_2 \in A$ and $b \in B$ such that $(b, a_1) \in f^{-1}$ and $(b, a_2) \in f^{-1}$. Then, $f(a_1) = b = f(a_2)$. However, f is one-to-one and thus $a_1 = a_2$. ∎

We will show that the converse of the above is also true; that is f has an inverse *if and only if* it is one-to-one and onto. Before doing so, we will prove two other theorems that will imply this.

Theorem 5.8 *Let $f : A \to B$ be a function and assume that $f^{-1} : B \to A$ is its inverse. Then, $f^{-1} \circ f = i_A$ and $f \circ f^{-1} = i_B$, where i_X denotes that identity relation on set X.*

Proof: Let $a \in A$ and let $b = f(a) \in B$. Then, $(a, b) \in f$ and $(b, a) \in f^{-1}$. Thus $(f^{-1} \circ f)(a) = f^{-1}(f(a)) = f^{-1}(b) = a = i_A(a)$. This proves that for all $a \in A$, $(f^{-1} \circ f)(a) = i_A(a)$, and so by Theorem 5.2 we have that $f^{-1} \circ f = i_A$. The proof for $f \circ f^{-1}$ is similar. ∎

Theorem 5.9 *Let $f : A \to B$ be a function.*

1. *If there exists a function $g : B \to A$ such that $g \circ f = i_A$ then f is one-to-one.*
2. *If there exists a function $g : B \to A$ such that $f \circ g = i_B$ then f is onto.*

Proof: We begin with the first part. Let $g : B \to A$ and assume that $g \circ f = i_A$. Let $a_1, a_2 \in A$ and assume that $f(a_1) = f(a_2)$. Applying g, we have that $g(f(a_1)) = g(f(a_2))$. However, since $g \circ f = i_A$ we have that $g(f(a_1)) = i_A(a_1) = a_1$ and $g(f(a_2)) = i_A(a_2) = a_2$, implying that $a_1 = a_2$. Thus, f is one-to-one.

Next, let $g : B \to A$ and assume that $f \circ g = i_B$. We prove that $\text{Ran}(f) = B$. Let $b \in B$ be an arbitrary element, and let $a \in A$ such that $g(b) = a$. By the assumption, $f \circ g = i_B$ and thus $f(g(b)) = b$. We conclude that $f(a) = b$ and thus $b \in \text{Ran}(f)$. We have proven that $B \subseteq \text{Ran}(f)$. By the definition of the range of a function, it follows that $\text{Ran}(f) \subseteq B$ and thus $\text{Ran}(f) = B$. By Theorem 5.5 we conclude that f is onto. ∎

We are now ready to conclude:

Theorem 5.10 *Let $f : A \to B$ be a function. The following statements are equivalent:*

1. *f is one-to-one and onto.*
2. *$f^{-1} : B \to A$ is a function.*
3. *There exists a function $g : B \to A$ such that $g \circ f = i_A$ and $f \circ g = i_B$.*

Proof:

$(1 \Rightarrow 2)$**:** This is exactly what is stated in Theorem 5.7.

$(2 \Rightarrow 3)$**:** Assume that f^{-1} exists, and let $g = f^{-1}$. Then, (3) follows directly from Theorem 5.8.

$(3 \Rightarrow 1)$**:** This is exactly what is stated in Theorem 5.9.

∎

Observe that the above theorem proves that the existence of a function $g : B \to A$ such that $g \circ f = i_A$ and $f \circ g = i_B$ implies the existence of an inverse of f. However, it does not state that for every such g it holds that $g = f^{-1}$. We now prove this stronger statement.

Theorem 5.11 *Let $f : A \to B$ and $g : B \to A$ be functions such that $g \circ f = i_A$ and $f \circ g = i_B$. Then, $g = f^{-1}$.*

Proof: By Theorem 5.10 we have that the inverse function $f^{-1} : B \to A$ exists. Thus, by Theorem 5.8 we have that $f^{-1} \circ f = i_A$. In addition, for all functions $h_1 : A \to B$ and $h_2 : B \to A$ it holds that $i_B \circ h_1 = h_1$ and $i_A \circ h_2 = h_2$ (exercise). Therefore:

$$g = i_A \circ g = (f^{-1} \circ f) \circ g = f^{-1} \circ (f \circ g) = f^{-1} \circ i_B = f^{-1},$$

where the 3rd equality follows from item (4) of Theorem 4.9. ∎

Example 5.12 *Define the function $f : \mathbb{R} \to \mathbb{R}^+$ (where $\mathbb{R}^+ = \{x \in \mathbb{R} \mid x \geq 0\}$) by $f(x) = x^2$. Does f have an inverse?*

It is easy to fall into the trap of defining $f^{-1}(y) = \sqrt{x}$. However, this is in fact not defined since every $y \in \mathbb{R}^+$ has *two* square roots over the reals: x and $-x$. Indeed, f is not one-to-one since $f(-x) = f(x)$ for every x. Thus, it *cannot* have an inverse.

The image and preimage of a set. We often wish to consider a function on a *subset* of inputs/outputs, and in particular, to relate to its image and preimage on such subsets. Let $f : A \to B$ be a function, and let $X \subseteq A$ and $Y \subseteq B$ be subsets of the domain and range of f, respectively. We define:

$$f(X) = \{f(x) \mid x \in X\} \quad \text{and} \quad f^{-1}(Y) = \{a \mid f(a) \in Y\}$$

For example, let $f : \mathbb{N} \to \mathbb{Z}$ be a function defined by $f(x) = -x$. Then, $f(\mathbb{N}) = \mathbb{Z}^-$ and $f^{-1}(\mathbb{N}) = \phi$. Observe that for every function $f : A \to B$ it holds that the function $f : A \to f(A)$ is onto.