Notes from How to Prove It

Julian Dominic

28 July 2022

Preface

I wrote these notes principally FOR understanding, they are meant for future reference for a refresher on what I have learnt. As such, certain definitions may not be exactly precise but are rephrased into simpler terms.
I am using the first edition of the book. ISBN 0-521-44663-5
Honestly, I don't have much to say, I just thought that a preface would be cool. Let's start our journey now.

Contents

1 Sentential Logic

1.1 Deductive reasoning and logical connectives

In an *argument*, we arrive at **valid** *conclusions* assuming that the *premises* are **true**.
Premises and conclusion are often referred to as conditions and outcomes respectively.
If all the premises are **true**, then the conclusion should be **true**. However, for the case where the conclusion is **false** while the premises are **true**, the argument is **invalid**.

1.1.1 Logical Operators

Symbol	Meaning	Description
$\vee$	OR	Disjunction
$\wedge$	AND	Conjunction
$\neg$	NOT	Negation

1.2 Truth tables

A truth table must be able to represent all possible combinations of the variables, premises and conclusions.

P	Q	$P \vee Q$
F	F	F
F	T	T
T	F	T
T	T	T

P	Q	$P \wedge Q$
F	F	F
F	T	F
T	F	F
T	T	T

P	$\neg P$
F	T
T	F

In this case, we see that our variables (or statements), P and Q have their individual column to assign a value – **True** or **False** – to them.
We use our logical operators to make a new statement from P and Q which can be $P \wedge Q$, and assign a value to the new statement.

It is important note that the number of variables will dictate the number of rows that the truth table will have. Construct a truth table for the following set of variables, $\{P\}$, $\{P, Q\}$, $\{P, Q, R\}$.
The pattern that we find is that as the number of variables increases, the number of rows increases two-fold.

$$\text{Number of Rows} = 2^{\text{Number of Variables}}$$

There are some special truth tables where the column for the conclusion always has the same value (either all *true* or all *false*) for every combination of the variables' values.

When the conclusion is always *true*, we say that the conclusion's statement is a **tautology**. Construct a truth table for $P \vee \neg P$.
Similarly, when the conclusion is always *false*, we say that the conclusion's statement is a **contradiction**. Construct a truth table for $P \wedge \neg P$.

> **Remark 1.1.** *Tautologies* and *Contradictions* are not the only laws that govern logic. Do see the logic document for more.

1.3 Variables and sets

1.3.1 Sets

A set is a collection of elements. The order of the elements in the set does not matter. If an element appears more than once, it is still the same set.

$$\{3, 7, 14\} \equiv \{7, 3, 14\} \equiv \{14, 3, 7, 7\}$$

When the set is infinite or has too many elemnts to list, we will define it explicitly. Suppose we have the following set P.

$$P = \{x \mid x \text{ is a prime number}\}$$

How we read $P = \{x|x\text{is a prime number}\}$ is "P is equal to the set of all x such that x is a prime number." Which also means that P contains all values of x that make the statement "x is a prime number" true. Some direct translations of the symbols into words would be (i) "$\{\}$" means "the set of", and (ii) "$|$" means "such that".

Sets like P have an **elementhood test** for the set; in this case, the *elementhood test* is being a prime number. Any value of x that makes the statement come out true, passes the test and is an element of the set.

Theorem 1.2 (Truth Set)

The **Truth set** of a statement $P(x)$ is the set of all values of x that make the statement $P(x)$ true. In other words, it is the set defined by using the statement $P(x)$ as the elementhood test:

$$\text{Truth set of } P(x) = \{x \mid P(x)\}$$

1.3.2 Understanding variables used in sets

There are two types of variables that can appear in a set; **Free variables** and **Bound variables**. *Free variables* are variables that will make the statement either *True* or *False* while *Bound variables* are variables whose values we do not need to know (they can be considered *dummy variables*). Lets consider the following example,

$$y \in \{x \mid x^2 < 9\}$$

For any number y, to verify $y \in \{x \mid x^2 < 9\}$, we have to check $y^2 < 9$. Since $y \in \{x \mid x^2 < 9\}$ is just a roundabout way of saying $y^2 < 9$, it follows that we do not need to care about the value of x. Rather, only the value of y is required. Thus, we can say that y is a *free variable* while x is a *bound variable.* As such, we can go further and replace x with any other variable except y because we do not need to care what x is. As such, it can even be $y \in \{w \mid w^2 < 9\}$ where y is *free* and w is *bound.* Notice that $x^2 < 9$ makes x a *free variable.* We can say that that statement $P(x)$ in $\{x \mid P(x)\}$ **binds** the variable x.

> **Remark 1.3.** In general, the statement $y \in \{x \mid P(x)\} \Rightarrow P(y)$ and $y \notin \{x \mid P(x)\} \Rightarrow \neg P(y)$.
> It is also important to note that $x \mid P(x)$ is not a statement. It is a set because of the curly brackets "{}"

Theorem 1.4 (Universe of Discourse)

The **Universe of Discourse**, U, is the set of all possible values for the variables. We can say things such as $\{x \in U \mid P(x)\}$: The set of all x in U such that $P(x)$. For a set that has the *universe of discourse* defined, an element of the set has to pass two tests, $x \in U$ and $P(x)$. Therefore, in general, $y \in \{x \in A \mid P(x)\} \Rightarrow y \in A \wedge P(y)$.
If $P(x)$ is false for every possible value of x, it yields a truth set with no elements. As such, we get the **empty set/null set**; $\emptyset$ or $\{\}$ where the contents inside the curly brackets are blank. For example,

$$\{x \in \mathbb{Z} \mid x \neq x\} = \emptyset = \{\}$$

> **Remark 1.5.** $\emptyset \neq \{\emptyset\}$. $\emptyset$ is a set while $\{\emptyset\}$ is a set of a set.

1.4 Operations on two sets

Theorem 1.6 (Intersection of sets)

The **Intersection** of sets – as the name suggests – will yield the set that contains elements that exists in both of the sets. Simply, it contains elements that the sets have in common.

$$A \cap B = \{x \mid x \in A \text{ and } x \in B\}$$

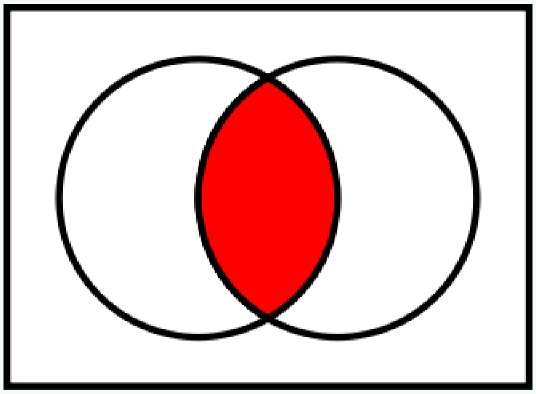

Figure 1: Source from Wikipedia

Theorem 1.7 (Disjoint)

A and B are **disjoint** if they have no elements in common; the **intersection** of the sets A and B does not exist – the set is empty. This is also known as **mutually exclusive**. Therefore, we can say that A and B are *mutually exclusive*.

$$A \cap B = \emptyset$$

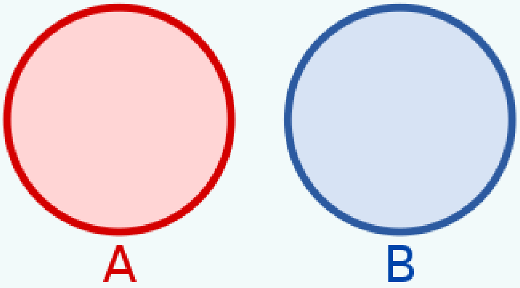

Figure 2: Source from Wikipedia

Theorem 1.8 (Union of two sets)

The **Union** of sets will yield the set that contains elements that come from any and all of the sets. Essentially, it is the amalgamation of all the elements from every set. It is important to note that in Mathematics, the word **or** is used 'inclusively'; Consider the example below, we want to get elements that are in either A or B or both. While in conversation, we may think of **or** as an exclusive term such as when making a decision between two choices.

$$A \cup B = \{x \mid x \in A \text{ or } x \in B\}$$

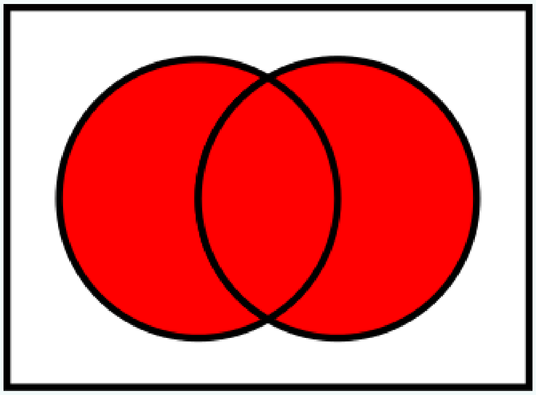

Figure 3: Source from Wikipedia

Theorem 1.9 (Difference of two sets)

The **Difference** of sets will yield the set that contains elements that are *exclusive* to set A. Exclusive is being used in its literal meaning here; we do not include an element that can be found in more than one set, the element has to be unique.

$$A \setminus B = \{x \mid x \in A \text{ and } x \notin B\}$$

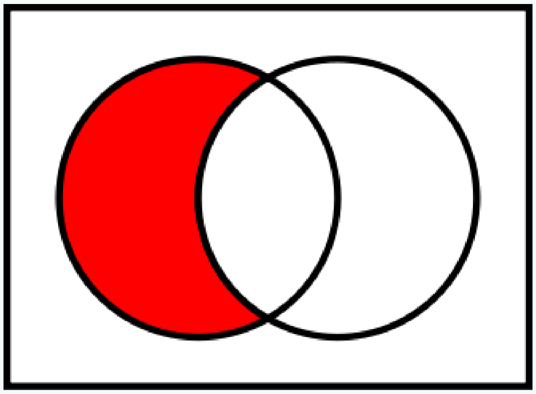

Figure 4: Source from Wikipedia

Theorem 1.10 (Symmetric Difference of two sets)

The **Symmetric Difference** of sets will yield the set that contains elements that are in either A or B but not both. To put it plainly, it is the set that contains elements that are exclusive to both A and B. You can think of it as the **union** of A and B without their **intersection**.

$$A \triangle B = (A \setminus B) \cup (B \setminus A)$$

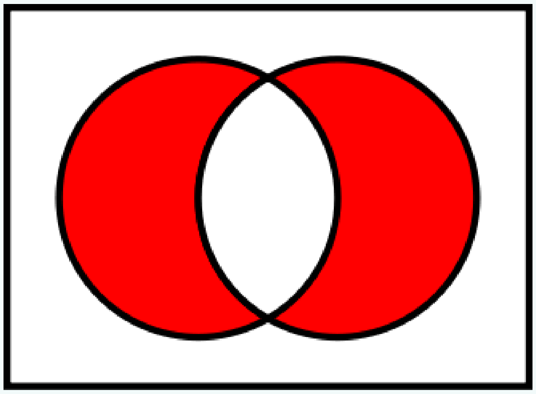

Figure 5: Source from Wikipedia

Theorem 1.11 (Subset)

A is a **subset** of B if every element of A is also an element of B. It is really just saying that B is the 'bigger brother' that contains A . There are also **proper subsets** where A is a subset of B but not equal to B (A cannot have every single element that B has).

$$A \subseteq B \quad \text{(Subset)}$$
$$A \subset B \quad \text{(Proper Subset)}$$

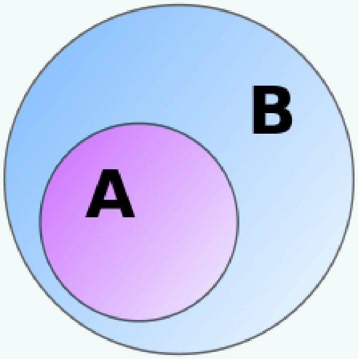

Figure 6: Source from Wikipedia

1.5 The conditional and biconditional connectives

1.5.1 Conditional Statement

Theorem 1.12 (Conditional Statement)

Conditional statements introduces a new logical connective, →. With reference to the expression below, $P \to Q$ is read as '**If** P **then** Q'. P and Q are known as the *antecedent* and *consequent* respectively.

$$P \to Q \ = \neg P \vee Q$$

P	Q	$P \to Q$
F	F	T
F	T	T
T	F	F
T	T	T

While using the equivalent formula $P \to Q \ = \ \neg P \vee Q$ is easier to calculate the values for the truth table, lets find the motivation to fill it in just by thinking about **if** and **then**.

The last row is painfully obvious. **If** P is *true* **then** Q is clearly *true.*
The third row is a little tricky but quite straightforward. There is no possible case for P to be *true* and Q to be *false* because **if** P is *true* **then** Q *must* be *true.* Therefore, the statement is *false.*
For the remaining rows, lets use an example to justify our answers. Let P stand for the statement that $x > 2$, and Q stand for the statement that $x^2 > 4$. For the first row, consider $x = 1$, it follows that $x^2 = 1 < 4$. I did not mention anything about an x-value that is less than or equal to 2; As such, it does not invalidate my

claim that '**If** $x > 2$ **then** $x^2 > 4$'. Therefore, the statement is *true*. Finally, for the second row, consider $x = -5$, it follows that $x^2 = 25 > 4$. Note, in a similar fashion for my justification for the first row, I still have not said anything that would invalidate my statement that earlier. Thus, the statement is *true*.

> **Remark 1.13.** One may question why not we just claim that $P \to Q$ is false for the first two rows? In our reasoning, we just said that our variables did not invalidate our statement so the 'truth'-value of our statement is actually unknown.
> To quote: "We accept a basic axiom of logic that tell us that every statement is either true or false, so we have to pick one. In mathematics, we find it more useful to take it to be true, but this is not necessary (for all)."

The **Converse** of any *conditional statement* is going in the opposite direction of its particular *conditional statement*. The thought process of considering the **converse** is *if* P *then* Q, but *if* Q *then* $P \equiv \boldsymbol{Q \to P}$?

The **Contrapositive** of any *conditional statement* is going in the opposite direction of its particular *conditional statement* **and** *negating* the variables. More often than not, it is often confused with the *converse*. This is because people often confuse the thought process of considering the **contrapositive** which would be seeing that $P \to Q \equiv \neg P \vee Q \equiv Q \vee \neg P \equiv \boldsymbol{\neg Q \to \neg P}$. One way to think about it is to break '**contrapositive**' into '*contra*' and '*positive*', as such, there should be no positive terms. Hence, there are negations on the variables.

Theorem 1.14 (Biconditional Statement)

$P \to Q$ and $Q \to P$ are not equivalent but more often than not, we want to say that both are true. This where **Biconditional statements** come in. We want to fufill two conditions at once (which is why it is called **biconditional**).
With reference to the example below, $P \longleftrightarrow Q$ can be read as mainly read as 'P **if and only if** Q' (some replace *if and only if* by *iff* for simplicity). It is read this way because of the way the **conditional** statements are formed which is $Q \to P$ is read as 'P if Q' and $P \to Q$ is read as 'P only if Q'.

$$\boldsymbol{P \longleftrightarrow Q} \equiv (P \to Q) \wedge (Q \to P) \equiv (P \to Q) \wedge (\neg P \to \neg Q)$$

> **Remark 1.15.** There are several other ways to which the **conditional** and **biconditional** statements can be read.
> $P \to Q$:
>
> - If P then Q.
> - P implies Q.
> - Q, if P.
> - P only if Q.
> - P is a sufficient condition for Q.
> - Q is a necessary condition for P.
>
> $P \longleftrightarrow Q$:
>
> - P if and only if Q or P iff Q.
> - P is a necessary and sufficient condition for Q.

2 Quantificational Logic

2.1 Quantifiers

Theorem 2.1 (Universal Quantifier)
To say that $P(x)$ is **true** for **every** value of x in the universe of discourse U, $P(x)$ is universally **true**.

$$\forall x P(x) : \text{For all } x, P(x).$$

Theorem 2.2 (Existential Quantifier)
To say that $P(x)$ is **true** for **at least one** value of x in the universe of discourse U.

$$\exists x P(x) : \text{There exists an } x \text{ such that } P(x)$$

To say that there is exactly one value of x in the universe of discourse U, such that $P(x)$.

$$\exists! x P(x) \equiv \exists x \left[P(x) \land \neg\exists y \left(P(y) \land y \neq x\right)\right]$$

2.2 Equivalences involving quantifiers

- $\neg\forall x P(x) \equiv \exists x \neg P(x)$
- $\neg\exists x P(x) \equiv \forall x \neg P(x)$
- $\{x \in U \mid P(x)\} \equiv \{x \mid P(x)\}$
- $\exists x \in A\ P(x) \equiv \exists x\,(x \in A \land P(x))$
- $\forall x \in A\ P(x) \equiv \forall x\,(x \in A \to P(x))$
- $A \subseteq B \equiv \forall x(x \in A \to B) \equiv \forall x \in A(x \in B)$
- $\forall x\,(P(x) \land Q(x)) \equiv \forall x P(x) \land \forall x Q(x)$
- $\forall x\,(P(x) \lor Q(x)) \not\equiv \forall x P(x) \lor \forall x Q(x)$
- $\exists x\,(P(x) \land Q(x)) \not\equiv \exists x P(x) \land \exists x Q(x)$
- $\exists x\,(P(x) \lor Q(x)) \equiv \exists x P(x) \lor \exists x Q(x)$

Consider the statement, “Nobody is perfect”, and express it in a logical form. It is often incorrectly written as $\neg\forall x P(x)$ where x is a person, and $P(x)$ is the statement that x is perfect. $\neg\forall x P(x)$ is saying that ‘Not everybody is perfect.’ which implies that there is at least one person that is not perfect (see the first item in the list above). When we see $\neg\forall x$, we immediately think of the complement of everyone which is none. However, that is wrong; ‘Not’ everyone is actually ‘someone’. Therefore, the answer should be $\forall x \neg P(x)$ or $\neg\exists x P(x)$ where they mean ‘Everyone is not perfect’ and ‘There is not a single person who is perfect’ respectively.

Consider the following, if $A = \emptyset = \{\}$, $\forall x \in A\ P(x)$ is vacuously true (there isn't a value of x for which $x \in A$ is true) and $\neg\forall x \in A\ P(x)$ is false.

$$\begin{aligned}\neg\forall x \in A\ P(x) &\equiv \neg\forall x(x \in A \to P(x))\\ &\equiv \neg\forall x(x \notin A \vee P(x))\\ &\equiv \exists x(x \in A \wedge \neg P(x))\\ &\equiv \exists x \in A\ \neg P(x)\end{aligned}$$

$\exists x \in A\ \neg P(x)$ says that 'There exists at least one value of x st. $\neg P(x)$'. However, since $A = \emptyset = \{\}$, there is no such value of x and therefore, the statement is false.

Remark 2.3. Changing the order of the quantifiers do not matter if they are the same type.

- $\forall x \forall y \equiv \forall y \forall x$
- $\exists x \exists y \equiv \exists y \exists x$

It is also important to note that $\forall x \in A$ and $\exists x \in A$ are bounded quantifiers. Consider $\forall x \in U\ (x \geq 0)$ where U can be $\mathbb{R}$ or $\mathbb{N}$.

2.3 More operations on sets

Consider the following,

- $S = \{x \mid \exists n \in \mathbb{N}\ (x = n^2)\} = \{n^2 \mid n \in \mathbb{N}\}$
- $x \in \{n^2 \mid n \in \mathbb{N}\} \equiv \exists n \in \mathbb{N}\ (x = n^2)$

Suppose $P = \{p_1, p_2, p_3, \ldots, p_100\}$, and we can represent the elements as p_i where $i \in I$. $I = \{1, 2, 3, \ldots, 100\} = \{i \in \mathbb{N} \mid 1 \leq i \leq 100\}$. Therefore, $P = \{p_i \mid i \in I\}$
I is called the **index set** because i is the **index**, and $\{p_i \mid i \in I\}$ is called an **indexed family**.

In general, Indexed Family: $A = \{x_i \mid i \in I\} = \{x \mid \exists i \in I\ (x = x_i)\} \Rightarrow x \in \{x_i \mid i \in I\} \equiv \exists i \in I\ (x = x_i)$

Example 2.4 (How to Prove It 2.3.1)

1. $y \in \{\sqrt[3]{x} \mid x \in \mathbb{Q}\} \equiv \exists x \in \mathbb{Q}\ (y = \sqrt[3]{x})$
2. $\{x_i \mid i \in I\} \subseteq A \Rightarrow x \in \{x_i \mid i \in I\} \subseteq A \equiv \forall x\,[\exists i \in I\ (x = x_i) \to x \in A] \equiv \forall i \in I\ (x_i \in A)$

Theorem 2.5 (Families of sets)

$\mathcal{F}$: Families of sets where $\mathcal{F}$ is a set of other sets. For example, $\mathcal{F} = \{A, B, C\}$ where A, B, C are sets.

Theorem 2.6 (Power Set)

Suppose A is a set. The **Power Set** of A is dentoed by $\mathcal{P}(A)$. $\mathcal{P}(A)$ is the set whose elements are all the subsets of A.

$$\mathcal{P}(A) = \{x \mid x \subseteq A\}$$

where x is a set.
For example, $A = \{7, 12\} \Rightarrow \mathcal{P}(A) = \{\emptyset, \{7\}, \{12\}, \{7, 12\}\}$
$\mathcal{P}(\emptyset) = \{\emptyset\}$

Remark 2.7. The empty set, $\emptyset$, is always a subset of every set including iteself, $\emptyset$.

Example 2.8 (How to Prove It 2.3.3)

1. $x \in \mathcal{P}(A)$ means that x is a subset of A.
   $\Rightarrow x \subseteq A \equiv \forall y(y \in x \to y \in A)$
2. $\mathcal{P}(A) \subseteq \mathcal{P}(B)$
   $\Rightarrow \forall x\,(x \in \mathcal{P}(A) \to x \in \mathcal{P}(B))$
   $\equiv \forall x\,[\forall y(y \in x \to y \in A) \to \forall y(y \in x \to y \in B)]$
3. $B \in \{\mathcal{P}(A) \mid A \in \mathcal{F}\}\}$
   $\equiv \exists A \in \mathcal{F}\ (B = \mathcal{P}(A))$
   $\equiv \exists A \in \mathcal{F}\ \forall x(x \in B \longleftrightarrow x \in \mathcal{P}(A))$
4. $x \in \mathcal{P}(A) \cap \mathcal{P}(B) \equiv x \in \mathcal{P}(A) \wedge x \in \mathcal{P}(B)$

Theorem 2.9 (Intersection of the Family)

Intersection of the Family: $\cap\boldsymbol{\mathcal{F}}$ contains the elements that all the sets in $\mathcal{F}$ have in common (given that $\mathcal{F} \neq \emptyset$). The elements must be in all sets A.

$$\cap\mathcal{F} = \{x \mid \forall A \in \mathcal{F}\ (x \in A)\} = \{x \mid \forall A(A \in \mathcal{F} \to x \in A)\}$$

Theorem 2.10 (Union of the Family)

Union of the Family: $\cup\boldsymbol{\mathcal{F}}$ contains all the possible elements that the sets in $\mathcal{F}$ have. The elements must be in at least 1 set A.

$$\cup\mathcal{F} = \{x \mid \exists A\ \ \in \mathcal{F}(x \in A)\} = \{x \mid \exists A(A \in \mathcal{F} \wedge x \in A\}$$

Consider the following, $\mathcal{F} = \{\{1, 2, 3, 4\}, \{2, 3, 4, 5\}, \{3, 4, 5, 6\}$.
It follows that, $\cap\mathcal{F} = \{3, 4\}$ and $\cup\mathcal{F} = \{1, 2, 3, 4, 5, 6\}$

Remark 2.11. Note: If A and B are the only two sets and $\mathcal{F} = \{A, B\}$, then $\cap\mathcal{F} = A \cap B$ and $\cup\mathcal{F} = A \cup B$

Consider the following, $x \in \cap\mathcal{F} \equiv \forall A(A \ \in \ \mathcal{F} \rightarrow x \ \in \ A)$.
Also consider the following, $x \in \cup\{\mathcal{P}(A) \mid A \ \in \ \mathcal{F}\}$. This means that x is an element of the union of the set of all power sets of A where A is an element of the family of sets $\mathcal{F}$. The union of all power sets is a large set that contains all of the subsets of A. For x to be an element of it, $x \in \mathcal{P}(A) \implies x \subseteq A$; x is one of the subsets of A. x is an element of at least one of the sets $\mathcal{P}(A)$ for $A \ \in \ \mathcal{F}$ (by definiton of union). It follows that $\exists A \in \mathcal{F}(x \in \mathcal{P}(A)) \equiv \exists A \in \mathcal{F}(x \subseteq A) \equiv \exists A \in \mathcal{F}\forall y(y \in x \rightarrow y \in A)$

Theorem 2.12 (Alternative Notation)

$$\mathcal{F} = \{A_i \mid i \in I\}$$
$$\cap\mathcal{F} = \cap_{i\in I}A_i = \{x \mid \forall i \in I(x \in A_i)\}$$
$$\cup\mathcal{F} = \cup_{i\in I}A_i = \{x \mid \exists i \in I(x \in A_i)\}$$

Example 2.13 (How to Prove It 2.3.7)

$I = \{1, 2, 3\}$, $A_1 = \{1, 2, 3, 4\}$, $A_2 = \{2, 3, 4, 5\}$, $A_3 = \{3, 4, 5, 6\}$

$$\cap_{i\in I}A_i = \{3, 4\}$$

$$\cup_{i\in I}A_i = \{1, 2, 3, 4, 5, 6\}$$

3 Proofs

3.1 Proof strategies

Theorem: If certain *assumptions* or *hypotheses* are**true**, the same *conclusion* must also be **true**. The *hypotheses* and *conclusion* often contain **free variables**. If we assign a value to them, it is called an **instance** (case) of the theorem. Therefore, for a theorem to be true, every instance must be true. It follows that if the hypotheses is **true** then the conclusion must be **true**.

Counterexample: Instance where the hypotheses are **true** but conclusion if **false**. Therefore, the theorem is **false**.

Theorem 3.1 (Goal: $P \to Q$; Direct)

To prove a goal of the form $P \to Q$, assume that P is **true** and then prove Q.
Before Proof strategy:

Givens (know assumed to be true)	Goal (statement to be proven)
˜ ˜	$P \to Q$

After Proof strategy:

Givens (know assumed to be true)	Goal (statement to be proven)
˜ ˜ P	Q

Form of the Final Proof:
Suppose P (is true). [Proof of Q (is true) goes here]. Therefore, $P \to Q$.

Consider the following statement, prove that if $0 < a < b$ then $a^2 < b^2$ where a and b are real numbers.

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

For a start, we assume $0 < a < b$ to be true, and use this assumption to prove $a^2 < b^2$.

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

We compare the inequalities $a < b$ and $a^2 < b^2$. To make $a < b$ sort of look like $a^2 < b^2$, we multiply both sides of the inequality by both a and b. We get $a^2 < ab$ and $ab < b^2$. Combining the two, we get $a^2 < b^2$. Therefore, if $0 < a < b$ then $a^2 < b^2$. □

Theorem 3.2 (Goal: $P \to Q$; Contrapositive)

To prove a goal of the form $P \to Q$, assume Q is **false** and prove that P is **false**.

$$P \to Q \equiv \neg Q \to \neg P$$

Before Proof strategy:

Givens (know assumed to be true)	Goal (statement to be proven)
~ ~	$P \to Q$

After Proof strategy:

Givens (know assumed to be true)	Goal (statement to be proven)
~ ~ $\neg Q$	$\neg P$

Form of the Final Proof:
Suppose Q is false. [Proof of $\neg P$ goes here]. Therefore, $P \to Q$.

Consider the statement, suppose a, b, and c are real numbers and $a > b$. Prove that if $ac \leq bc$ then $c \leq 0$.

Givens	Goal
$a, b, c \in \mathbb{R}$	$c \leq 0$
$a > b$	
$ac \leq bc$	

We will prove the contrapositive. Suppose $c > 0$. $a > b$ follows that by multiplying c to the inequality, $ac > bc$ which is the contra of $ac \leq bc$. Therefore, if $ac \leq bc$ then $c \leq 0$. □

Remark 3.3.

- $P \to Q$: modus ponens
- $\neg Q \to \neg P$: modus tollens

3.2 Proofs involving negations and conditionals

Usually easier to prove a positive statement than a negative statement. It is helpful to re-express a goal of the form $\neg P$ before proving it.

Theorem 3.4 (Goal: $\neg P$)

To prove a goal of the form $\neg P$, if possible, re-express the goal in some other ofrm and then use one of the proof stategies for this other goal form.

Consider the statement, $A \cap C \subseteq B$ and $a \in C$, prove that $a \notin A \setminus B$. After some manipulation, $a \notin A \setminus B \equiv \neg(a \in A \setminus B) \equiv \neg(a \in A \wedge a \notin B) \equiv a \notin A \vee a \in B \equiv a \in A \rightarrow a \in B$.
Suppose $a \in A$. Since $a \in C$, then $a \in A \cap C$. But then since $A \cap C \subseteq B$, it follows that $a \in B$. Therefore, it cannot be these case that a is an element of A and not B, thus, $a \in A \setminus B$. □

Theorem 3.5 (Goal: $\neg P$; Contradiction)

Assume P is true and try to reach a contradiction (usually of one of the givens). Once you have reached a contradiction, you can conclude that P must be false (because the given must be true!). Before Proof strategy:

Givens (know assumed to be true)	Goal (statement to be proven)
~	$\neg P$
~	

After Proof strategy:

Givens (know assumed to be true)	Goal (statement to be proven)
~	Contradiction
~	
P	

Form of the Final Proof:
Suppose P is true. [Proof of Contradiction goes here]. Therefore, P is false.

Consider the statement, prove that if $x^2 + y = 13$ and $y \neq 4$ then $x \neq 3$.

Givens	Goal
$x^2 + y = 13$	$x \neq 3$
$y \neq 4$	

At this current state, suppose $x^2 + y = 13$ and $y \neq 4$. [Proof of $x \neq 3$ goes here]. Therefore, if $x^2 + y = 13$ and $y \neq 4$, then $x \neq 3$.

Givens	Goal
$x^2 + y = 13$	Contradiction
$y \neq 4$	
$x \neq 3$	

Suppose $x^2 + y = 13$ and $y \neq 4$. Suppose $x = 3$. [Proof of Contradiction goes here]. Thus, $x \neq 3$. Therefore, if $x^2 + y = 13$ and $y \neq 4$, then $x \neq 3$.

Therefore, for the final proof, suppose $x^2 + y = 13$ and $y \neq 4$. Suppose $x = 3$. When $x = 3, (3)^2 + y = 13 \Rightarrow y = 13 - 9 = 4$. But this contradicts the condition that $y \neq 4$. Therefore, $x \neq 3$. Thus, if $x^2 + y = 13$ and $y \neq 4$, then $x \neq 3$.

Theorem 3.6 (Given: $\neg P$; Contradiction)

If you are doing a proof by contradiction, try making P your goal. If you can prove P (is true), then the proof is complete, bceause P (is true) contradicts the given P. Before Proof strategy:

Givens (know assumed to be true)	Goal (statement to be proven)
$\neg P$ ~ ~	contradiction

After Proof strategy:

Givens (know assumed to be true)	Goal (statement to be proven)
$\neg P$ ~ ~	P

Form of the Final Proof:
[Proof of P goes here]. Since we already know $\neg P$, this is a contradiction.

In many cases, the logical form of a statement can be discovered by writing out the definition of some mathematical word or symbol that occurs in the statement.

Consider the statement, suppose A, B, and C are sets, $A \setminus B \subseteq C$, and x is anything at all. Prove that if $x \in A \setminus C$ then $x \in B$.

Givens	Goal
$A \setminus B \subseteq C$	$x \in B$
$x \in A \setminus C$	

Since $x \in B$ cannot be broken down further, we will proceed with a proof by contradiction.

Givens	Goal
$A \setminus B \subseteq C$ $x \in A \setminus C$ $x \notin B$	Contradiction

At this current state, suppose $x \in A \setminus C$. Suppose $x \notin B$. [Proof of Contradiciton goes here]. Therefore, $x \in B$. Thus, if $x \in A \setminus C$, then $x \in B$.
However, it is still not immediately obvious on how to the contradiciton. Let us break down the givens and see what we can find. Notice that the new given ($x \notin C$) has the form $\neg P$. Using the strategy where a given has $\neg P$.

Givens	Goal
$A \setminus B \subseteq C$ $x \in A$ $x \notin C$ $x \notin B$	$x \in C$

At this current state, suppose $x \in A \setminus C$. This means that $x \in A$ and $x \notin C$. Suppose $x \notin B$. [Proof of $x \in C$ goes here]. This contradicts $x \notin C$. Therefore, $x \in B$. Thus, if $x \in A \setminus C$, then $x \in B$.
Therefore, for the final proof, suppose $x \in A \setminus C$. This means that $x \in A$ and $x \notin C$. Suppose $x \notin B$. Since $x \in A$ and $x \notin B$, it follows that $x \in A \setminus B$. Thus, $A \setminus B \subseteq C$ follows that $x \in C$. This contradicts $x \notin C$. Therefore, $x \in B$. Thus, if $x \in A \setminus C$, then $x \in B$. □

To use a given of the form $\neg P$: If possible, re-express this given in some other form where you get a positive statement. (Though, you can still use the contradiction method either way; Proof by Contradiction is usually a 'last' resort option).

Theorem 3.7 (Given: $P \to Q$; Rules of Inference)

If you are also given P, or if you can prove that P is true, then you can use this given to conclude that Q is true. Since $P \to Q$ is equivalent to $\neg Q \to \neg P$ (by contrapositive law), if you can conclude Q is false, you can use this given to conclude that P is false.

There is no 'fixed' proof strategy for the Givens and Goal table here. Instead, we will be using an example below.

Consider the statement, suppose $P \to (Q \to R)$, prove that $\neg R \to (P \to \neg Q)$.

Givens	Goal
$P \to (Q \to R)$	$\neg R \to (P \to \neg Q)$
$P \to (Q \to R)$ $\neg R$	$P \to \neg Q$
$P \to (Q \to R)$ $\neg R$ P	$\neg Q$
$P \to (Q \to R)$ $\neg R$ P $Q \to R$	$\neg Q$

For the final proof, suppose $P \to (Q \to R)$. Suppose $\neg R$. Suppose P, it follows that $Q \to R$. Since $Q \to R \equiv \neg R \to \neg Q$, and $\neg R$, it follows that $\neg Q$. Therefore, $P \to \neg Q$. Thus, $\neg R \to (P \to \neg Q)$. □

3.3 Proofs involving quantifiers

If you can give a proof of the goal $P(x)$ that would work no matter what x was, then you can conclude that $\forall x P(x)$ must be true. To make sure that your proof would work *for any* value of x, it is important to start your proof with no assumptions about x. We can say this by saying that x must be arbitrary.

Theorem 3.8 (Goal: $\forall x P(x)$)

To prove a goal of the form $\forall x P(x)$, let x stand for an arbitrary object and prove $P(x)$. The letter x must be a new variable in the proof. If x is already being used in the proof to stand for something, then you must choose an unused variable (for example, y), to stand for the arbitrary object and prove it ($P(y)$).
Before Proof strategy:

Givens (know assumed to be true)	Goal (statement to be proven)
~ ~	$\forall x P(x)$

After Proof strategy:

Givens (know assumed to be true)	Goal (statement to be proven)
~ ~	$P(x)$

Form of the Final Proof:
Let x be arbitrary. [Proof of $P(x)$ goes here]. Since x was arbitrary, we can conclude that $\forall x P(x)$ (is true).

Consider the following statement, suppose A, B, and C are sets, and $A \setminus B \subseteq C$. Prove that $A \setminus C \subseteq B$.

Givens	Goal
$A \setminus B \subseteq C$	$A \setminus C \subseteq B \equiv \forall x(x \in A \setminus C \to x \in B)$
$A \setminus B \subseteq C$	$x \in A \setminus C \to x \in B$

For the final proof, let x be arbitrary. Suppose $x \in A \setminus C$. This means that $x \in A$ and $x \notin C$. Suppose $x \notin B$, it follows that $x \in A \setminus B$. Since $x \in A \setminus B$, $x \in C$. But this contradicts $x \notin C$. Therefore, $x \in B$. Hence, if $x \in A \setminus C$ then $x \in B$. Since x was arbitrary, we can conclude that $\forall x(x \in A \setminus C \to x \in B)$ so $A \setminus C \subset B$. □

Theorem 3.9 (Goal: $\exists x P(x)$)

To prove a goal of the form $\exists x P(x)$, find a value for which $P(x)$ will be true. Let $x =$ that value. Prove $P(x)$ for this value of x. Do note that, x should be a new variable. If it is already being used, use another variable, and use $\exists y P(y)$ and prove $P(y)$.
Before Proof strategy:

Givens (know assumed to be true)	Goal (statement to be proven)
~ ~	$\exists x P(x)$

After Proof strategy:

Givens (know assumed to be true)	Goal (statement to be proven)
~ ~ $x =$ value	$P(x)$

Form of the Final Proof:
Let $x =$ value. [Proof of $P(x)$ goes here]. Thus, $\exists x P(x)$.

Consider the following statement, prove that for every real number x, if $x > 0$, then there is a real number y such that $y(y + 1) = x$.

We start by solving for y. $y^2 + y - x = 0 \Rightarrow y = \frac{-1 \pm \sqrt{1+4x}}{2}$. Now, we just need to let $y =$ one of the values to prove that $y(y + 1) = x$.
For the final proof, let x be an arbitrary real number, and suppose $x > 0$. Let $y = \frac{-1+\sqrt{1+4x}}{2}$ which is **real** since $x > 0$. It follows that,

$$\begin{aligned} y(y+1) &= \left(\frac{-1+\sqrt{1+4x}}{2}\right)\left(\frac{-1+\sqrt{1+4x}}{2}+1\right) \\ &= \left(\frac{-1+\sqrt{1+4x}}{2}\right)\left(\frac{1+\sqrt{1+4x}}{2}\right) \\ &= \frac{1+4x-1}{4} \\ &= x \end{aligned}$$

Thus, $\exists y\,[y(y + 1) = x]$. Therefore, $x > 0 \to \exists y\,[y(y + 1) = x]$. Since x was arbitrary, we can conclude that $\forall x\,(x > 0 \to \exists y\,[y(y + 1) = x])$. □

Theorem 3.10 (Given: $\exists x P(x)$)

To use a given of the form $\exists x P(x)$, introduce a new variable x_0 into the proof to stand for an object for which $P(x_0)$ is true. This means that you can now assume $P(x_0)$ is true. This is called the rule of inference: **Existential Instantiation**.
Please note that you can assume that x_0 stands for some object for which $P(x_0)$ is true **BUT** you cannot assume anything else about x_0. This means that you do not get to choose a particular value to plug in for x.

Theorem 3.11 (Given: $\forall x P(x)$)

To use a given of the form $\forall x P(x)$, introduce any value for x. Use this given to conclude that $x = a$ and hence, $P(a)$ is true. This is called the rule of inference: **Universal Instantiation**.

Consider the following statement, suppose $\mathcal{F}$ and $\mathcal{G}$ are families of sets and $\mathcal{F} \cap \mathcal{G} \neq \emptyset$; Prove that $\cap\mathcal{F} \subseteq \cup\mathcal{G}$.

Givens	Goal
$\mathcal{F} \cap \mathcal{G} \neq \emptyset$	$\cap\mathcal{F} \subseteq \cup\mathcal{G}$
$\exists A(A \in \mathcal{F} \cap \mathcal{G})$	$\forall x\,(x \in \cap\mathcal{F} \rightarrow x \in \cup\mathcal{G})$
$\exists A(A \in \mathcal{F} \cap \mathcal{G})$	$\forall x\,(\forall A \in \mathcal{F}(x \in A) \ \rightarrow\ \exists A \in \mathcal{G}(x \in A))$
$\exists A(A \in \mathcal{F} \cap \mathcal{G})$ $\forall A \in \mathcal{F}(x \in A)$	$\exists A \in \mathcal{G}(x \in A)$
$A_0 \in \mathcal{F} \cap \mathcal{G} \equiv A_0 \in \mathcal{F} \wedge A_0 \in \mathcal{G}$ $\forall A \in \mathcal{F}(x \in A)$	$\exists A \in \mathcal{G}(x \in A)$

Since $A_0 \in \mathcal{F}$, we can conclude that $x \in A_0$ from $\forall A \in \mathcal{F}(x \in A)$.
For the final proof, suppose $x \in \cap\mathcal{F}$. Since $\mathcal{F} \cap \mathcal{G} \neq \emptyset$, we can let A_0 be an element of $\mathcal{F} \cap \mathcal{G}$. Thus, $A_0 \in \mathcal{F}$ and $A_0 \in \mathcal{G}$. Since $x \in \cap\mathcal{F}$ and $A_0 \in \mathcal{F}$, it follows that $x \in A_0$. We also know that $A_0 \in \mathcal{G}$. Therefore, $x \in \cup\mathcal{G}$. □