Inference Rules and Proof

This document will acquaint you with various basic arguments that will be frequently used in the course. I write $p_1, p_2, \cdots, p_n \therefore q$ to mean the argument with premises (i.e. assumptions) $p_1, p_2, \cdots, p_n$ and with conclusion q.

Not only do we want to make arguments, we want to make correct arguments. An argument is *valid* when the premises together imply the conclusion. In other words, the argument $p_1, p_2, \cdots, p_n \therefore q$ is valid when the statement $(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \implies q$ is a tautology; this formally expresses the concept that when the premises of the argument hold, the conclusion must also hold. This is fundamental to good reasoning.

Common (Valid) Argument Forms

The following are the fundamental valid arguments; these will inspire most of our proof methods in this course.

- $P \implies Q, P \therefore Q$ (Modus Ponens)
- $P \implies Q, \neg Q \therefore \neg P$ (Modus Tollens)
- $P \vee Q, \neg P \therefore Q$ (Disjunctive Syllogism)
- $P \implies Q, Q \implies R \therefore P \implies R$ (Hypothetical Syllogism)
- $P \iff Q, Q \iff R \therefore P \iff R$ (Biconditional Syllogism)
- $P \implies (Q \wedge (\neg Q)) \therefore \neg Q$ (Reductio Ad Absurdum)
- $P \implies R, Q \implies R, P \vee Q \therefore R$ (Case Elimination)
- $P, Q \therefore P \wedge Q$ (Conjunctive Addition)
- $P \wedge Q \therefore P$ (Conjunctive Simplification)
- $P \therefore P \vee Q$ (Disjunctive Addition)
- $P \wedge (\neg P) \therefore Q$ (Explosion)

Exercise. *Show that the above argument forms are valid (via proposition algebra or a truth table).*

Basic Proof Methods

In this section we will briefly survey some methods of proof inspired by the argument forms above.

Direct Proof

When attempting to prove an implication $P \implies Q$, fundamentally one assumes P and then proceeds (via previously established results and basic logic) to derive the conclusion Q. This is loosely inspired by Modus Ponens.

Proposition. *Let A and B be sets. If $A \subseteq B$, then* $\text{pow}(A) \subseteq \text{pow}(B)$.

Proof. Let A and B be sets and assume $A \subseteq B$. Let $S \in \text{pow}(A)$ be arbitrary. Thus $S \subseteq A$ by definition of the power set. As $S \subseteq A$ and $A \subseteq B$ we have $S \subseteq B$; thus $S \in \text{pow}(B)$ by definition of the power set. Hence $\text{pow}(A) \subseteq \text{pow}(B)$ by definition of the subset relation, which completes the proof. □

Notice that in the above proof we followed the following rough template:

1. State our assumptions/premises ("assume $A \subseteq B$").
2. Reason from definitions and prior results (bulk of the proof).
3. Clearly state our conclusion ("hence $\text{pow}(A) \subseteq \text{pow}(B)$").

This is the minimum necessary structure for a direct proof of an implication.

Contrapositive Proof

When attempting to prove an implication $P \implies Q$, we might prefer to work with the contrapositive statement $(\neg Q) \implies (\neg P)$. One directly proves the contrapositive statement. Implications are equivalent to their contrapositives, so this proves the original statement. This is loosely inspired by Modus Tollens.

Proposition. *Let A, B, and C be sets. If $A \subseteq B$ or $A \subseteq C$, then $A \subseteq B \cup C$.*

Proof. Let A, B, and C be sets. Proceeding by contrapositive, assume $A \not\subseteq B \cup C$. Thus there is an element $x \in A$ such that $x \notin B \cup C$. As $x \notin B \cup C$, we have $x \notin B$ and $x \notin C$. Thus $A \not\subseteq B$ and $A \not\subseteq C$. At this point, we have shown that $A \not\subseteq B \cup C$ implies either $A \not\subseteq B$ or $A \not\subseteq C$. Hence the original statement follows by contrapositive. □

Notice that in the above proof we followed the following rough template:

1. Tell the reader that we are making a contrapositive proof ("proceeding by contrapositive").
2. Follow the template for a direct proof of the contrapositive statement.
3. Clearly state that our conclusion follows from the contrapositive.

This is the minimum necessary structure for a contrapositive proof of an implication.

String of Implications

When attempting to prove an implication $P \implies Q$, it may be more convenient to write a string of implications beginning with our assumption P and ending with our conclusion Q. This is inspired by Hypothetical Syllogism.[1]

Proposition. *Let A, B, and C be sets. If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$.*

Proof. Let A, B, and C be sets. Assume $A \subseteq B$ and $B \subseteq C$. We have the following string of implications for all x:

$$\begin{aligned} x \in A &\implies x \in B && \text{(by } A \subseteq B\text{)} \\ &\implies x \in C && \text{(by } B \subseteq C\text{)} \end{aligned}$$

Hence $A \subseteq C$ and the original statement holds. □

Notice that in the above proof we followed the following rough template:

1. State our assumptions.
2. Tell the reader we will use a string of implications ("we have the following string of implications").
3. Clearly state our conclusion.

This is the minimum necessary when making a string of implications.

String of Biconditionals

When attempting to prove a biconditional $P \iff Q$, we can take two general approaches; either prove $P \implies Q$ and $Q \implies P$ separately by other methods, or we may write a string of biconditionals beginning with our assumption P and ending with our conclusion Q. This is inspired by Biconditional Syllogism.

Proposition. *For all sets A, B, and C we have $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.*

Proof. Let A, B, and C be sets. We have the following string of equivalent statements for all x:

$$\begin{aligned} x \in A \cap (B \cup C) &\iff (x \in A) \wedge (x \in B \cup C) && \text{(defn of intersection)} \\ &\iff (x \in A) \wedge [(x \in B) \vee (x \in C)] && \text{(defn of union)} \\ &\iff [(x \in A) \wedge (x \in B)] \vee [(x \in A) \wedge (x \in C)] && (\wedge\vee\text{-distribution}) \\ &\iff (x \in A \cap B) \vee (x \in A \cap C) && \text{(defn of intersection)} \\ &\iff x \in (A \cap B) \cup (A \cap C) && \text{(defn of union)} \end{aligned}$$

Hence $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ by definition of set equality. □

[1] The distinction here is somewhat artificial; these are direct proofs with shorter layout.

Notice that in the above proof we followed the following rough template:

1. State our assumptions.
2. Tell the reader we will use a string of biconditionals ("we have the following string of equivalences").
3. Clearly state our conclusion.

This is the minimum necessary when making a string of biconditionals.

Proof by Cases

When proving a statement, it is sometimes very useful to break the proof into two or more separate proofs based on some more specific assumptions coming from a known true disjunctive statement. This allows us more information to use in the proof, which often can help make a proof easier. This is inspired by Case Elimination.

Proposition. *Let A, B, and C be sets. If $A \subseteq C$ and $B \subseteq C$, then $A \cup B \subseteq C$.*

Proof. Let A, B, and C be sets, and assume $A \subseteq C$ and $B \subseteq C$. Let $x \in A \cup B$ be arbitrary; thus either $x \in A$ or $x \in B$. We proceed by cases.

Case 1: If $x \in A$, then by $A \subseteq C$ we have $x \in C$.

Case 2: If $x \in B$, then by $B \subseteq C$ we have $x \in C$.

Note that in all possible cases we have $x \in C$. Hence $A \cup B \subseteq C$ as desired. □

Notice that in the above proof we followed the following rough template:

1. Identify a true disjunction ("either $x \in A$ or $x \in B$").
2. Tell the reader that we will proceed to analyze multiple cases.
3. Analyze each of the disjuncts to arrive at the desired conclusion in each case separately.
4. Clearly state our conclusion.

This is the minimum necessary when making a proof by cases.

Proof by Contradiction

A proof by contradiction appeals to the idea that every statement is either true or false, and not both. Suppose we want to prove a statement P. In this method of proof we assume the negation $\neg P$ and then proceed by our usual rules of good reasoning to derive an absurdity (a statement of the form $Q \wedge (\neg Q)$). Having done so, we can conclude that the statement we assumed ($\neg P$) must be false, and thus that $\neg(\neg P) \equiv P$ is true. This style of proof is inspired by Reductio Ad Absurdum.

Proposition. *Let A and B be sets. If $A \subseteq B$, then $A \cup B = B$.*

Proof. Let A and B be sets and assume $A \subseteq B$. As $A \cup B = \{x \mid x \in A \text{ or } x \in B\}$, we see that $x \in B$ implies $x \in A \cup B$; thus $B \subseteq A \cup B$. Assume to the contrary that $A \cup B \not\subseteq B$. In particular there is an element $x_0 \in A \cup B$ such that $x_0 \notin B$; thus $x_0 \in A$ by definition of the set union. Thus $x_0 \in B$ by our assumption $A \subseteq B$; this yields $x_0 \in B$ and $x_0 \notin B$, which is absurd. Thus no such x_0 can exist, yielding $A \cup B \subseteq B$. Hence $A \cup B = B$ as desired. □

Notice that in the above proof we followed the following rough template:

1. Signal to the reader that we will make a proof by contradiction ("assume to the contrary").
2. Use good reasoning to arrive at a contradiction.
3. Clearly state the contradiction, and signal that it is a contradiction.
4. Clearly state our conclusion from the contradiction before proceeding.

This is the minimum necessary when making a proof by contradiction.

Notice that there are better ways to prove the statement above; it is possible to prove this statement directly (indeed, it's quite a bit easier). We'll talk more about this a little later.

General Notes on Proving Statements

Here we will make some remarks on proof format and style; we also address a few common mistakes.

Existential Versus Universal Proof

Here is a statement, together with a false proof.

Proposition. *Let A and B be sets. The set $A = (A \cap B) \cup (A - B)$.*

Just to reiterate: the following is a BAD proof, and would receive no credit.

FALSE "PROOF". Let $A = \{1, 2, 3, 4\}$ and $B = \{2, 4, 5\}$. Then $A \cap B = \{2, 4\}$ and $A - B = \{1, 3\}$, so $(A \cap B) \cup (A - B) = \{2, 4\} \cup \{1, 3\} = \{1, 2, 3, 4\} = A$. Thus $A = (A \cap B) \cup (A - B)$ as desired. □

But why is this a bad proof? We showed $A = (A \cap B) \cup (A - B)$, right?
WRONG.
We showed that two very specific sets A and B satisfied $(A \cap B) \cup (A - B)$; the statement wants us to show that FOR ALL possible sets A and B. There is an implicit universal quantifier in the above statement. In particular, a more formal rewriting of this statement above is as follows:

$$\forall \text{ sets } A, B[A = (A \cap B) \cup (A - B)]$$

Now we see exactly where we went wrong; we didn't show that the relationship holds for all A and B like the statement wanted us to–we just gave an example.
To actually prove the statement, we need to give a more general argument. We can make several arguments for this statement; the first below is one that shows $A \subseteq (A \cap B) \cup (A - B)$ and $(A \cap B) \cup (A - B) \subseteq A$ directly. You should try to make your own proof using a string of equivalences.

Correct Proof. Let A and B be sets. We will show that $A = (A \cap B) \cup (A - B)$.
Let $x \in A$ be arbitrary. Either $x \in B$ or $x \notin B$; we proceed by cases.
Case 1: If $x \in B$, then $x \in A \cap B$ because $x \in A$ and $x \in B$; thus $x \in (A \cap B) \cup (A - B)$ because $x \in A \cap B$.
Case 2: If $x \notin B$, then $x \in A - B$ because $x \in A$ and $x \notin B$; thus $x \in (A \cap B) \cup (A - B)$ because $x \in A - B$.
Hence in either case we have $x \in (A \cap B) \cup (A - B)$; as $x \in A$ was arbitrary we see $A \subseteq (A \cap B) \cup (A - B)$.
Let $x \in (A \cap B) \cup (A - B)$ be arbitrary. Either $x \in A \cap B$ or $x \in A - B$; we proceed by cases.
Case 1: If $x \in A \cap B$, then $x \in A$ by definition of intersection.
Case 2: If $x \in A - B$, then $x \in A$ by definition of set difference.
Hence in either case we have $x \in A$; as $x \in (A \cap B) \cup (A - B)$ was arbitrary we see $(A \cap B) \cup (A - B) \subseteq A$.
Hence we have $A = (A \cap B) \cup (A - B)$ as desired. □

When proving a statement which is universally quantified, we MUST give a proof which always works, not just in some specific instances. A single example will NEVER prove a universally quantified statement.
Similarly, when asked to prove an existential statement (or DISPROVE a universal one) we just need to find one example. This is because a THERE EXISTS type statement is true as long as we can find a single example.

Proposition. *There is a set with five elements.*

Proof. The set $\{1, 2, 3, 4, 5\}$ has five elements, as desired. □

One must be very careful not to mix up one's quantifiers and their meanings...