We will cover these parts of the book (8th edition):

1.5-1.7
1.8.1-1.8.4

Nested Quantifiers

- When one quantifier is within the scope of another. Such as
  - $\forall x \exists y (x + y = 0)$

Statement	When True?	When False
$\forall x \forall y P(x, y)$ $\forall y \forall x P(x, y)$	p(x,y) is true for every pair x,y.	There is a pair x,y for which p(x,y) is false.
$\forall x \exists y P(x, y)$	For every x there is a y for which p(x,y) is true.	There is an x such that p(x,y) is false for every y
$\exists x \forall y P(x, y)$	There is an x for which p(x,y) is true for every y	For every x there is a y for which p(x,y) is false.
$\exists x \exists y P(x, y)$ $\exists y \exists x P(x, y)$	There is a pair x,y for which p(x,y) is true.	p(x,y) is false for every pair x,y.

UMASS BOSTON

Rules of Inference

- Proofs in mathematics are valid arguments that establish the truth of mathematical statements. By an **argument**, we mean a sequence of statements that end with a conclusion. By **valid**, we mean that the conclusion, or final statement of the argument, must follow from the truth of the preceding statements, or **premises**, of the argument.
- Consider "If you have a current password, then you can log onto the network.". Use p to represent "you have a current password" and q to represent "you can log onto the network".

$$\begin{array}{l} p \to q \\ p \\ \hline \therefore q \end{array}$$

- Where $\therefore$ is the symbol that denotes "therefore". When both $p \to q$ and p are true, we know that q must also be true. We say this form of argument is **valid** because whenever all its premises are true, the conclusion must also be true.

Rules of Inference

- How to show an argument is valid?
  1. Use a truth table → a boring approach!
  2. First stablish the validity of rules of inference. Then use them to construct more complicated valid argument forms.
- Rules of inference provide the justification of the steps used in a proof.
- One important rule is called modus ponens or the law of detachment. It is based on the tautology $(p \land (p \to q)) \to q$. We write it in the following way:

$$\begin{array}{r} p \to q \\ p \\ \hline \therefore q \end{array}$$

The two hypotheses p and $p \to q$ are written in a column, and the conclusion below a bar.

Rules of Inference

Rule of Inference	Name
p, $p \to q$, $\therefore q$	Modus ponens
$\neg q$, $p \to q$, $\therefore \neg p$	Modus tollens
$p \to q$, $q \to r$, $\therefore p \to r$	Hypothetical syllogism
$p \vee q$, $\neg p$, $\therefore q$	Disjunctive syllogism

Rule of Inference	Name
p, $\therefore p \vee q$	Addition
$p \wedge q$, $\therefore p$	Simplification
p, q, $\therefore p \wedge q$	Conjunction
$p \vee q$, $\neg p \vee r$, $\therefore q \vee r$	Resolution

Arguments

- **Example:**
- "If 101 is divisible by 3, then 101^2 is divisible by 9. 101 is divisible by 3. Consequently, 101^2 is divisible by 9."
- Although the argument is **valid**, its conclusion is **incorrect**, because one of the hypotheses is false ("101 is divisible by 3.").
- If in the above argument we replace 101 with 102, we could correctly conclude that 102^2 is divisible by 9.

Arguments

- Which rule of inference was used in the last argument?

- p: “101 is divisible by 3.”
- q: “101^2 is divisible by 9.”

$$\begin{array}{l} p \\ p \to q \\ \hline \therefore q \end{array}$$

Modus ponens

Unfortunately, one of the hypotheses (p) is false. Therefore, the conclusion q is incorrect.

Arguments

- **Another example:**
- "If it rains today, then we will not have a barbeque today. If we do not have a barbeque today, then we will have a barbeque tomorrow.
Therefore, if it rains today, then we will have a barbeque tomorrow."
- This is a **valid** argument: If its hypotheses are true, then its conclusion is also true.

Arguments

- Let us formalize the previous argument:
- p: “It is raining today.”
- q: “We will not have a barbecue today.”
- r: “We will have a barbecue tomorrow.”
- So the argument is of the following form:

$$\begin{array}{r} p \to q \\ q \to r \\ \hline \therefore p \to r \end{array}$$

Hypothetical syllogism

Arguments

- **Another example:**

- Gary is either intelligent or a good actor.
- If Gary is intelligent, then he can count from 1 to 10.
- Gary can only count from 1 to 2.
- Therefore, Gary is a good actor.

- i: “Gary is intelligent.”
- a: “Gary is a good actor.”
- c: “Gary can count from 1 to 10.”

Arguments

- i: “Gary is intelligent.”
  a: “Gary is a good actor.”
  c: “Gary can count from 1 to 10.”

- Step 1: $\neg c$ Hypothesis
- Step 2: $i \rightarrow c$ Hypothesis
- Step 3: $\neg i$ Modus Tollens Steps 1 & 2
- Step 4: $a \vee i$ Hypothesis
- Step 5: a Disjunctive Syllogism Steps 3 & 4

- Conclusion: **a** (“Gary is a good actor.”)

UMASS BOSTON

Arguments

- **Yet another example:**

- If you listen to me, you will pass CS 220.
- You passed CS 220.
- Therefore, you have listened to me.

- Is this argument valid?

- No, it assumes $((p \rightarrow q) \land q) \rightarrow p$.
- This statement is not a tautology. It is false if p is false and q is true. This type of incorrect reasoning is called the fallacy of affirming the conclusion.

Rules of Inference for Quantified Statements

$$\frac{\forall x\, p(x)}{\therefore\ p(c)\ if\ c \in U}$$

Universal instantiation

$$\frac{p(c) \text{ for an arbitrary } c}{\therefore\ \forall x\, p(x)}$$

Universal generalization

$$\frac{\exists x\, p(x)}{\therefore\ p(c) \text{ for some element } c}$$

Existential instantiation

$$\frac{p(c) \text{ for some element } c}{\therefore\ \exists x\, p(x)}$$

Existential generalization

Rules of Inference for Quantified Statements

- **Example:**

- Every UMB student is a genius.
- George is a UMB student.
- Therefore, George is a genius.

- U(x): “x is a UMB student.”
- G(x): “x is a genius.”

Rules of Inference for Quantified Statements

- The following steps are used in the argument:

- Step 1: $\forall x\, (U(x) \rightarrow G(x))$ Hypothesis
- Step 2: $U(\text{George}) \rightarrow G(\text{George})$ Univ. instantiation using Step 1

Step 3: $U(\text{George})$ Hypothesis
Step 4: $G(\text{George})$ Modus ponens using Steps 2 & 3

$$\frac{\forall x\, p(x)}{\therefore\ p(c)\ if\ c \in U}$$

Universal instantiation

Mathematical Reasoning

- We need **mathematical reasoning** to
  - determine whether a mathematical argument is correct or incorrect and
  - construct mathematical arguments.

- Mathematical reasoning is not only important for conducting **proofs** and **program verification**, but also for **artificial intelligence** systems (drawing inferences).

Terminology

- An **axiom** is a basic assumption about mathematical structures that needs no proof.
- We can use a **proof** to demonstrate that a particular statement is true. A proof consists of a sequence of statements that form an argument.
- The steps that connect the statements in such a sequence are the **rules of inference**.
- Cases of incorrect reasoning are called **fallacies**.
- A **theorem** is a statement that can be shown to be true. Less important theorems sometimes are called propositions.

Terminology

- A **lemma** is a simple theorem used as an intermediate result in the proof of another theorem.

- A **corollary** is a proposition that follows directly from a theorem that has been proved.

- A **conjecture** is a statement whose truth value is unknown. It is a statement that is being proposed to be a true statement, usually on the basis of some partial evidence. Once it is proven, it becomes a theorem.

UMASS BOSTON

Proving Theorems

- **Direct proof:**
- An implication $p \rightarrow q$ can be proved by showing that if p is true, then q is also true.

- **Example:** Give a direct proof of the theorem "If n is odd, then n^2 is odd."

- **Idea:** Assume that the hypothesis of this implication is true (n is odd). Then use rules of inference and known theorems to show that q must also be true (n^2 is odd).

UMASS BOSTON

Proving Theorems

- n is odd.

- Then $n = 2k + 1$, where k is an integer.

- Consequently, $n^2 = (2k + 1)^2$.
- $= 4k^2 + 4k + 1$
- $= 2(2k^2 + 2k) + 1$

- Since n^2 can be written in this form, it is odd.

Proving Theorems

- **Indirect proof (Contrapositive):**

- An implication $p \rightarrow q$ is equivalent to its **contra-positive** $\neg q \rightarrow \neg p$. Therefore, we can prove $p \rightarrow q$ by showing that whenever q is false, then p is also false.

- **Example:** Give an indirect proof of the theorem "If 3n + 2 is odd, then n is odd."

- **Idea:** Assume that the conclusion of this implication is false (n is even). Then use rules of inference and known theorems to show that p must also be false (3n + 2 is even).

Proving Theorems

- n is even.
- Then $n = 2k$, where k is an integer.
- It follows that $3n + 2 = 3(2k) + 2$
- $= 6k + 2$
- $= 2(3k + 1)$
- Therefore, $3n + 2$ is even.
- We have shown that the contrapositive of the implication is true, so the implication itself is also true (If $3n + 2$ is odd, then n is odd).

Proving Theorems

- **Indirect proof (contradiction):**
- Suppose we want to prove that a statement p is true. Furthermore, suppose that we can find a contradiction q such that $\neg p \rightarrow q$ is true. Because q is false, but $\neg p \rightarrow q$ is true, we can conclude that $\neg p$ is false, which means that p is true.

- **Example:** Show that at least four of any 22 days must fall on the same day of the week.

- **Idea:** Let p be "At least four of 22 chosen days fall on the same day of the week". Suppose $\neg p$ is true. So at most three of the 22 days fall on the same day. But each week has 7 days. So it's not possible.

Proving Theorems

- **Proofs of equivalence:**
- To prove $p \leftrightarrow q$, we show that $p \rightarrow q$ and $q \rightarrow p$ are both true. $(p \leftrightarrow q) \leftrightarrow (p \rightarrow q) \wedge (q \rightarrow p)$

- **Counterexamples:**
- To show that $\forall x P(x)$ is false, we need only find a counterexample, that is, an example x for which $P(x)$ is false.

Mistakes in Proofs

- 1. Some mistakes result from the introduction of steps that do not logically follow from those that precede it.
- **Example:** Proof of 1=2

"Proof": We use these steps, where a and b are two equal positive integers.

Step	**Reason**
1. $a = b$	Given
2. $a^2 = ab$	Multiply both sides of (1) by a
3. $a^2 - b^2 = ab - b^2$	Subtract b^2 from both sides of (2)
4. $(a - b)(a + b) = b(a - b)$	Factor both sides of (3)
5. $a + b = b$	Divide both sides of (4) by $a - b$
6. $2b = b$	Replace a by b in (5) because $a = b$ and simplify
7. $2 = 1$	Divide both sides of (6) by b

Mistakes in Proofs

- **Solution:**
- Every step is valid except for step 5, where we divided both sides by $a - b$. The error is that $a - b$ equals zero; division of both sides of an equation by the same quantity is valid as long as this quantity is not zero.

Mistakes in Proofs

- 2. Some incorrect arguments are based on a fallacy called **begging the question**. This fallacy occurs when one or more steps of a proof are based on the truth of the statement being proved. In other words, this fallacy arises when a statement is proved using itself, or a statement equivalent to it. That is why this fallacy is also called **circular reasoning**.

- **Example:** Proof of n is an even integer whenever n^2 is an even integer.
- Proof: Suppose that n^2 is even. Then $n^2 = 2k$ for some integer k. Let $n = 2l$ for some integer l. This shows that n is even.

Mistakes in Proofs

- **Solution:**
- This argument is incorrect. The statement “let $n = 2l$ for some integer l” occurs in the proof. No argument has been given to show that n can be written as $2l$ for some integer l. This is circular reasoning because this statement is equivalent to the statement being proved, namely, “n is even.” The result itself is correct; only the method of proof is wrong.

UMASS BOSTON

Exhaustive Proof and Proof by Cases

- **Exhaustive Proof:**
- Proving by examining all possibilities. For example prove that $(n+1)^3 \geq 3^n$ if n is a positive integer with $n \leq 4$.

- **Proof by cases:**
- Must cover all the possible cases that arise in a theorem.
- Example in next slide

Proving by Cases

- For every positive integer n, n(n + 1) is even.

- **Idea:** Let us first show that the product of an even number m and an odd number n is always even:

- $m = 2k$
- $n = 2p + 1$
- $mn = 2k(2p + 1) = 4kp + 2k$
- $mn = 2(2kp + k)$

- Since k and p are integers, (2kp + k) is an integer as well, and we have shown that mn is even.

Proving by Cases

- The remainder of the proof becomes easy if we separately consider each of the two main situations that can occur:
- **Case I:** n is even.
- Then n(n + 1) means that we multiply an even number with an odd one. As shown above, the result must be even.
- **Case II:** n is odd.
- Then n(n + 1) means that we multiply an odd number with an even one. As shown above, the result must be even.
- Since there are no other cases, we have proven that n(n + 1) is always even.

Existence and Uniqueness Proofs

- **Existence Proofs:**
- A proof of a proposition of the form $\exists x P(x)$.
  1. Constructive: Finding a witness "a" such that $P(a)$ is true.
  2. Nonconstructive: Prove that $\exists x P(x)$ is true in some other way. For example by contradiction.

- Example for constructive: Show that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways.
  - **Solution:** $1729 = 10^3 + 9^3 = 12^3 + 1^3$
- Example for nonconstructive: Show that there exist irrational numbers x and y such that x^y is rational.
  - **Solution:** Consider the number $\sqrt{2}^{\sqrt{2}}$. So $x = \sqrt{2}, y = \sqrt{2}$ or $x = \sqrt{2}^{\sqrt{2}}, y = \sqrt{2}$.

Existence and Uniqueness Proofs

- **Uniqueness Proofs:**
- A proof of a proposition of the form $\exists! xP(x)$. So it has 2 parts:
  1. Existence: An element with this property exits.
  2. Uniqueness: If x and y both have this property, then x=y
- Example: Show that if a and b are real numbers and $a \neq 0$, then there is a unique real number r such that $ar + b = 0$.
  - **Solution: (Existence)** $r = -\frac{b}{a}$
  - **(Uniqueness)** suppose s is another real number with this property. So we have $ar + b = as + b \Rightarrow ar = as \Rightarrow r = s$