CSCE 222
Discrete Structures for Computing

David Kebo Hougninou

Proofs

Chapter 1
Proof

A proof is a valid argument that establishes the truth of a mathematical statement.

Rules of Inference

To prove mathematical statements, we must give valid arguments for them:
1. Start with statements we already know are true
2. Deduce new true statements from the ones we already know
3. Reach a conclusion

Rules of Inference:
The means for deducing new true statements.
Rules of Inference

e.g.
1. If you know your eCampus password, then you can see your grade.
2. You know your eCampus password.
3. Conclusion: You can see your grade.

If $p \rightarrow q$ is true and $p$ is true, then $q$ is true.

Rules of inference
Templates
Rules of Inference

Rules of inference have templates for constructing arguments.

1. Start with a collection of propositions, $p_1, p_2, \ldots, p_n$: the premises
2. End with another proposition, $q$: the conclusion.

Let’s review!

Rules of Inference

- Modus Ponens
- Modus Tollens
- Hypothetical syllogism
- Disjunctive syllogism
- Addition
- Simplification
- Conjunction
- Resolution
Modus Ponens

* Latin for: *mode that affirms*

The tautology \([p \land (p \rightarrow q)] \rightarrow q\) is the basis of the rule of inference.

\[
p \\
p \rightarrow q \\
\hline \\
\therefore q
\]

Modus Tollens

* Latin for: *method of denying*

\[
\neg q \\
p \rightarrow q \\
\hline \\
\therefore \neg p \\
(\neg q \land (p \rightarrow q)) \rightarrow \neg p
\]
Hypothetical syllogism

\[
\begin{align*}
p &\rightarrow q \\
q &\rightarrow r \\
\therefore p &\rightarrow r \\
(p \rightarrow q \land q \rightarrow r) &\rightarrow (p \rightarrow r)
\end{align*}
\]

Disjunctive syllogism

\[
\begin{align*}
p \lor q \\
\neg p \\
\neg p &\lor q \\
\therefore q \\
[(p \lor q) \land \neg p] &\rightarrow q
\end{align*}
\]
Addition

\[ p \]
\[ \quad \rightarrow \]
\[ \therefore p \lor q \]

\[ p \rightarrow p \lor q \]

Simplification

\[ p \land q \]
\[ \quad \rightarrow \]
\[ \quad \rightarrow \]
\[ \therefore p \]

\[ p \land q \rightarrow p \]
Conjunction

\[
\begin{align*}
p \\
q \\
\hline
\therefore p \land q
\end{align*}
\]
\[[(p) \land (q)] \to p \land q\]

Resolution

\[
\begin{align*}
p \lor q \\
\neg p \lor r \\
\hline
\hline
\therefore q \lor r
\end{align*}
\]
\[[(p \lor q) \land (\neg p \lor r)] \to q \lor r\]

e.g.:
Either you know the password or you use your fingerprint.
Either you don’t know password or you buy a new laptop.
\therefore Either you use your fingerprint or you buy a new laptop.
Fallacies

• Fallacy = error in reasoning that results in an invalid argument
• Types of fallacies:
  1. Converse Error
  2. Inverse Error

Converse Error

\[ p \rightarrow q \]
\[ q \]
\[ \therefore p \]

Let \( p = \) it rains, \( q = \) the grass is wet

If it rains, then the grass will be wet
The grass is wet
\[ \therefore \text{It rained} \]

The grass could be wet from another source
Converse Error – Truth Table

<table>
<thead>
<tr>
<th>p</th>
<th>q</th>
<th>p → q</th>
<th>q</th>
<th>p</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
</tr>
</tbody>
</table>

Observe the critical rows where the conclusion is false. This argument form is invalid (Fallacy).

Inverse Error

\[ \begin{align*}
    p \rightarrow q \\
    \neg p \\
    \hline \\
    \therefore \neg q
\end{align*} \]

Let \( p = \) it rains, \( q = \) the grass is wet
If it rains, then the grass will be wet
It is not raining
\[ \therefore \text{The grass is not wet} \]
The grass could be wet from another source
## Inverse Error – Truth Table

<table>
<thead>
<tr>
<th>Premises</th>
<th>Conclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>p</td>
<td>q</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
</tr>
</tbody>
</table>

Observe the critical rows where the conclusion is false. This argument form is invalid (Fallacy).

## Example

Is the following argument valid or invalid?

- If you invest in the Bitcoin, then you get rich.
- You did not invest in Bitcoin.
- Therefore, you did not get rich. 😞
Example

Is the following argument **valid** or **invalid**? 😐
- If you read chapter 1, then you will get 100 for the quiz.
- You got 100 for the quiz.
- Therefore, you have read chapter 1.

Application of rules of Inference

Suppose we know these facts about a program:

1. x is not equal to 5 and x is greater than y.
2. If y is prime, then x equals 5.
3. If y is not prime, then z is odd.
4. If z is odd, then z is less than x.

Can we conclude that: **z is less than x**?
Let’s use propositional variables instead:

\[ p: \text{“x equals 5”} \]
\[ q: \text{“x is greater than y”} \]
\[ r: \text{“y is prime”} \]
\[ s: \text{“z is odd”} \]
\[ t: \text{“z is less than x”} \]

Formalize the premises as propositions:

(a) \( \neg p \land q \)
(b) \( r \rightarrow p \)
(c) \( \neg r \rightarrow s \)
(d) \( s \rightarrow t \)

The conclusion is the proposition t.
Activity

Show that the following argument is valid:

- It is not sunny and it is colder than yesterday.
- We will go swimming only if it is sunny.
- If we do not go swimming, then we will take a canoe trip.
- If we take a canoe trip, then we will be home by sunset.
∴
We will be home by sunset.

Methods of proving theorems

• Direct proofs
• Indirect proofs
  1. Proof by contraposition
  2. Proof by contradiction
Direct Proof

A direct proof is a proof that shows that a conditional statement $p \rightarrow q$ is true by showing that if $p$ is true then $q$ is true.

Use:
- rules of inference
- axioms
- logical equivalences
to prove that $q$ must also be true.

Remember: Start with premises and end with a conclusion!

Direct Proof Template

1. Suppose variable(s) are particular but arbitrarily chosen type of numbers.

2. Use definitions, substitutions, and rules of algebra to prove that $q$ is true

3. Conclude
Assumptions

• The basic laws of algebra apply
• The following properties of equality apply:
  – $A = A$
  – If $A = B$, then $B = A$
  – If $A = B$ and $B = C$, then $A = C$
• The set of all integers $(\mathbb{Z})$ is \textit{closed} under addition, subtraction, and multiplication

Direct Proof Example

Prove the following statement:
"The sum of any two \textit{odd} integers is \textit{even}"

Direct Proof Example

Proof:
- Suppose \( m \) and \( n \) are any particular but arbitrarily chosen odd integers.
- By definition of odd, there exist integers \( r \) and \( s \) such that:
  \[ m = 2r+1 \text{ and } n = 2s+1 \]
- By substitution:
  \[ m + n = (2r+1) + (2s + 1) \]
  \[ m + n = 2r + 2s + 2 \]
  \[ m + n = 2(r + s + 1) \]
  \( u = r + s + 1 \) is an integer (Because \( \mathbb{Z} \) is closed under addition)

Therefore, the sum of any two odd integers is even!

Activity

Prove the following statement:
"For all integers \( m \), if \( m \) is even then \( 3m+5 \) is odd"
Activity solution

Prove the following statement: "For all integers $m$, if $m$ is even then $3m+5$ is odd"

By definition of an even number: $m = 2k$, $k \in \mathbb{Z}$

By substitution: $3m + 5 = 6k + 5 = 6k + 4 + 1 = 2(3k + 2) + 1$

$3k + 2$ is an integer (Because $\mathbb{Z}$ is closed under addition and multiplication)

Therefore, For all integers $m$, if $m$ is even then $3m+5$ is odd

---

Even and Odd Integers

We are looking at integers (set $\mathbb{Z}$)

An integer $n$ is even iff $n =$ twice some integer
Formally: $n$ is even $\iff \exists \; k \in \mathbb{Z} \mid n = 2k$

An integer $n$ is odd iff $n =$ twice some integer plus one
Formally: $n$ is odd $\iff \exists \; k \in \mathbb{Z} \mid n = 2k + 1$
Activity

a) Prove that \(-10\) is even?

b) If \(x\) and \(y\) are integers, prove that \(4x + 2y + 1\) is odd

Activity solution

a) Prove that \(-10\) is even?

i.e., is there an integer \(k\) such that \(-10 = 2k\)?
\[-10 = 2(-5)\]
\[-5 \in \mathbb{Z}\]
Therefore, \(-10\) is even

b) If \(x\) and \(y\) are integers, prove that \(4x + 2y + 1\) is odd

i.e., is there an integer \(k\) such that \(4x + 2y + 1 = 2k + 1\)?
\[4x + 2y + 1 = 2(2x + y) + 1\]
\[k = 2x + y\] is an integer (Because \(\mathbb{Z}\) is closed under addition and multiplication)

Therefore, if \(x\) and \(y\) are integers, then \(4x + 2y + 1\) is odd
Prime and Composite Integers

• An integer \( n \) is prime iff \( n > 1 \) and for all positive integers \( r \) and \( s \), if \( n = rs \), then either \( r \) or \( s \) equals \( n \)

\[
n \text{is prime} \iff (n>1) \land (\forall \ r,s \in \mathbb{Z}^+, (n=rs) \rightarrow (r = 1 \land s=n) \lor (s=1 \land r=n))
\]

• An integer \( n \) is composite iff \( n > 1 \) and there exists some integers \( r,s \) (\( 1 < r < n \), \( 1 < s < n \)) where \( n = rs \)

\[
n \text{is composite} \iff (n>1) \land (\exists \ r,s \in \mathbb{Z}^+, (1<r<n, 1<s<n) \land n = rs)
\]

Example

Prove that 3 is a prime number
a) Prove that 2 is a prime number

An integer n is prime iff n>1 and for all positive integers r and s, if n = rs, then either r or s equals n
Step 1: 2 > 1
Step 2: if 2 = rs, then r=2, n=1 or r=1, n=2
So 2 is prime

b) Prove that 4 is a composite number

Step 1: 4> 1
Step 2: 4 = 4 * 1 = 2 * 2
So 2 is a composite number
Proof by contraposition

A proof by contraposition is a proof that shows that a conditional statement \( p \rightarrow q \) is true by showing that if \( q \) is false then \( p \) is false.

\[ p \rightarrow q \equiv \neg q \rightarrow \neg p \]

A proof by contraposition is an indirect proof.
An indirect proof does not start with the premises to end with a conclusion.

Proof by contraposition template

1. Take \( \neg q \) is a premise.
2. Use rules of inference, axioms, definitions, theorems to prove that \( \neg p \) is true.
3. Conclude.
Proof by contraposition Example

Prove the following statement (n is an integer):
“if $3n + 2$ is odd then $n$ is odd”

Proof by contraposition Solution

“if $3n + 2$ is odd then $n$ is odd”

$p$: $3n + 2$ is odd; $q$: $n$ is odd; $p \rightarrow q$

Let's prove that: $\neg q \rightarrow \neg p$

$\neg q$: $n$ is even

$n = 2k$ (Definition of an even number)

$3n + 2 = 3(2k) + 2 = 2(3k + 1)$ (By Substitution)

$3k + 1$ is an integer (Because $\mathbb{Z}$ is closed under multiplication and addition)

Therefore $3n + 2$ is even ($\neg p$)

$\therefore$ “if $3n + 2$ is odd then $n$ is odd”
**Proof by contradiction**

A *proof by contraposition* is a proof that shows that a statement $p$ is true by showing that $\neg p$ is false.

We prove that $\neg p$ cannot be true (contradiction), thus $p$ is true.

A proof by contraposition is an *indirect proof*.

---

**Proof by contradiction template**

1. Take $\neg P$ is a premise.

2. Use rules of inference, axioms, definitions, theorems to prove that $\neg P$ is false.

3. Conclude.
Proof by contradiction Example

Prove the following statement (n is an integer):
“if 3n + 2 is odd then n is odd”

Proof by contradiction Solution

“if 3n + 2 is odd then n is odd”
p: 3n + 2 is odd; q: n is odd; p → q

Let's prove that: ¬(p → q) is a contradiction
p → q ≡ ¬p ∨ q so, ¬(p → q) ≡ p ∧ ¬q
p: 3n + 2 is odd and ¬q: n is even
n = 2k (Dy Definition of an even number)
3n + 2 = 3(2k) + 2 = 2(3k + 1) (By Substitution)
3k + 1 is an integer (Because Z is closed under multiplication and addition)
Therefore 3n + 2 is even. This is a contradiction!
∴ “if 3n + 2 is odd then n is odd”
Proving Existential Statements

\( \exists x \in D \) such that \( Q(x) \) is true \iff \( Q(x) \) is true for \textit{at least one} \( x \) in \( D \).

One way to prove this is to find an \( x \) in \( D \) that makes \( Q(x) \) true.

Another way is to give a set of directions for finding such an \( x \).

Both of these methods are called \textit{constructive proofs of existence}.

Example

Prove: \( \exists \) an even integer \( n \) that can be written as a sum of two composite numbers

We need to find at least one \( n \) where this is true.

Composite numbers are 4, 6, 8, 9,10,12, ...

4 + 6 = 10, let \( n = 10 \).

So the statement is true.
Disproving Universal Statements by Counterexample

To disprove a statement means to show that it is false.

Disprove: $\forall x \text{ in } D, \text{ if } P(x) \text{ then } Q(x)$

Showing that this statement is false is equivalent to showing that its negation is true.

The negation of the statement is existential: $\exists x \text{ in } D \text{ such that } P(x) \text{ and not } Q(x)$.

Example

Given the following statement:

$\forall x,y \in \mathbb{R}, (x^2 = y^2) \rightarrow (x = y)$

Find a counterexample to disprove this statement

$\exists x,y \in \mathbb{R} \mid (x^2 = y^2) \land \sim (x = y)$

So let $x = -2$, $y = 2$

$x^2 = y^2, (-2)^2 = 4, 2^2 = 4, \text{ so } 4 = 4$

But, $-2 \neq 2$, so $\sim (x = y)$
Example

Disprove the following statement by giving a counterexample:

“For all integers n, if n is odd then (n-1)/2 is odd.”

Example solution

Disprove the following statement by giving a counterexample:

“For all integers n, if n is odd then (n-1)/2 is odd.”

There exists n = 5 such that (5-1)/2 is even
Proving Universal Statements

How to prove a universal statement?

The majority of mathematical statements to be proved are universal.

∀x ∈ D, if P(x) then Q(x)

When D is finite or when only a finite number of elements satisfy P(x), such a statement can be proved by the method of exhaustion.

Method of Exhaustion

∀n ∈ Z, if n is even and 4 ≤ n ≤ 16, then n can be written as a sum of two prime numbers. Prime numbers are 2,3,5,7,11,13

<table>
<thead>
<tr>
<th>n</th>
<th>sum of primes</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>2+2</td>
</tr>
<tr>
<td>6</td>
<td>3+3</td>
</tr>
<tr>
<td>8</td>
<td>3+5</td>
</tr>
<tr>
<td>12</td>
<td>5+7</td>
</tr>
<tr>
<td>14</td>
<td>7+7</td>
</tr>
<tr>
<td>16</td>
<td>5+11</td>
</tr>
</tbody>
</table>
Application to Computer Science

- We could exhaustive run a program to test all cases.
- For large data sets, it would take a long time (many years even with the fastest computer)
- We need a shortcut to verify the operation of our program.
- By using the method of generalizing from the generic particular, we can then use the method of direct proof to prove universal statements.

End