# 4. Proof Methods

Proof methods are essential both in mathematics and computer science.

Applications include:

- verifying that computer programs are correct
- establishing that operating systems are secure
- making inferences in artificial intelligence
- showing that system specifications are consistent

Reading assignment: Up to Section 4.1 of the zyBook



## TERMINOLOGY

rules of inference

common proof methods

proofs by induction

## TERMINOLOGY: Propositions and Proofs 4.3

***PROPOSITION***: *statement that can be shown to be true*

If everyone in this class is a genius
and if you are a student in this class
then you are a genius.

*premises*: everyone in this class is a genius; you are a student in this class

*conclusion*: you are a genius

***PROOF***: *valid argument that establishes the truth of the proposition*

1. Everyone in this class is a genius
2. You are a student in this class
3. If you are a student in this class then you are a genius
4. You are a genius

*sequence of statements that ends with the conclusion*

The argument is *valid* if each statement is a premise or follows from the truth of the preceding statements.





## TERMINOLOGY: Propositions, Conjectures, Axioms 4.4

***theorem***
an important proposition

***lemma***
a proposition helpful in the proof of a more important proposition

***corollary***
a proposition that can be easily derived from another proposition

***conjecture***
a statement that is believed to be true
but for which no proof has been found yet

***axiom***
a statement that cannot be proved or disproved
but that is taken to be true (and can be used in proofs)

**NOTE: Axioms form the basic structure of a mathematical theory.**

terminology

## RULES OF INFERENCE

common proof methods

proofs by induction



## RULES OF INFERENCE: Definition 4.6

A ***rule of inference*** is a tautology of the form
$(part_1 \wedge part_2 \wedge \ldots \wedge part_n) \rightarrow part_{n+1}$

If $part_1$, $part_2$, ..., $part_n$ are true
then $part_{n+1}$ must be true!

Notation:

$$\begin{array}{l} part_1 \\ part_2 \\ \ldots \\ part_n \\ \hline \therefore\ part_{n+1} \end{array}$$

or

*premises*

$$\begin{array}{l} part_1,\ part_2,\ \ldots,\ part_n \\ \hline \therefore\ part_{n+1} \end{array}$$

*conclusion*

$[p \wedge (p \rightarrow q)] \rightarrow q$
is a rule of inference
called ***modus ponens***.

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

Reading assignment: Up to Section 4.3 of the zyBook

## RULES OF INFERENCE: Importance 4.7

Rules of inference are building blocks for proofs.
They are basic tools for establishing the truth of statements.





## RULES OF INFERENCE and Propositional Logic 4.8

$$\frac{p \qquad p\rightarrow q}{\therefore\ q}$$

Name: ***modus ponens***
Associated tautology: $[p\wedge(p\rightarrow q)]\rightarrow q$

$$\frac{\neg q \qquad p\rightarrow q}{\therefore\ \neg p}$$

Name: ***modus tollens***
Associated tautology: $[\neg q\wedge(p\rightarrow q)]\rightarrow\neg p$

$$\frac{p\rightarrow q \qquad q\rightarrow r}{\therefore\ p\rightarrow r}$$

Name: ***hypothetical syllogism***
Associated tautology: $[(p\rightarrow q)\wedge(q\rightarrow r)]\rightarrow(p\rightarrow r)$

$$\frac{p\vee q \qquad \neg p}{\therefore\ q}$$

Name: ***disjunctive syllogism***
Associated tautology: $[(p\vee q)\wedge\neg p]\rightarrow q$

$$\frac{p}{\therefore\ p\vee q}$$

Name: ***addition***
Associated tautology: $p\rightarrow(p\vee q)$

$$\frac{p\wedge q}{\therefore\ p}$$

Name: ***simplification***
Associated tautology: $(p\wedge q)\rightarrow p$

$$\frac{p \qquad q}{\therefore\ p\wedge q}$$

Name: ***conjunction***
Associated tautology: $(p\wedge q)\rightarrow(p\wedge q)$

$$\frac{p\vee q \qquad \neg p\vee r}{\therefore\ q\vee r}$$

Name: ***resolution***
Associated tautology: $[(p\vee q)\wedge(\neg p\vee r)]\rightarrow(q\vee r)$

## RULES OF INFERENCE and Predicate Logic 4.9

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

Name:
***universal instantiation***

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

Name:
***universal generalization***

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

Name:
***existential instantiation***

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

Name:
***existential generalization***





## RULES OF INFERENCE: Are You a Genius? 4.10

***PROPOSITION***: If everyone in this class is a genius
and if you are a student in this class
then you are a genius.

***PROOF***: *argument*

1. Everyone in this class is a genius
2. You are a student in this class
3. If you are a student in this class then you are a genius
4. You are a genius

The *argument* is valid because its *form* is valid.

*argument's form*

Let the set of all students in the world be the universe of x, let S be the predicate defined by "x is a student in this class" and let G be the predicate defined by "x is a genius".

| | |
|---|---|
| 1. $\forall x, (S(x) \to G(x))$ | Premise |
| 2. S(you) | Premise |
| 3. S(you)→G(you) | Universal instantiation from 1. |
| 4. G(you) | Modus ponens from 2. and 3. |

## RULES OF INFERENCE: Fallacies 4.11

A ***fallacy*** is a form of incorrect reasoning.

This $\begin{array}{l} p \rightarrow q \\ q \\ \hline \therefore p \end{array}$ is NOT a valid rule of inference.

Using it is making the fallacy of *affirming the conclusion*.

This $\begin{array}{l} p \rightarrow q \\ \neg p \\ \hline \therefore \neg q \end{array}$ is NOT a valid rule of inference.

Using it is making the fallacy of *denying the premise*.

## COMMON METHODS: Direct Proofs 4.13

***PROPOSITION***: Let $n$ be an integer.
If $n$ is even then $n^2$ is even.

***PROOF***: Assume $n$ is even.
Then, ......
Therefore, ......
Obviously, ......
......
Therefore, ......
Clearly, ......
......
In other words, $n^2$ is even

*from the premises to the conclusion*





## COMMON METHODS: Proofs by Contraposition 4.14

Based on the fact that $p \to q \equiv \neg q \to \neg p$
A ***proof by contraposition*** of $p \to q$ is a direct proof of $\neg q \to \neg p$

***PROPOSITION***: Let $n$ be an integer.
If $n^2$ is even then $n$ is even.

***PROOF***: Assume $n$ is NOT even.
Then, ......
Therefore, ......
Therefore, ......
......
In other words, $n^2$ is NOT even.

## COMMON METHODS: Proofs by Contradiction 4.15

Based on the fact that $p \equiv \neg p \rightarrow (q \wedge \neg q)$
A ***proof by contradiction*** of $p$ is a direct proof of $\neg p \rightarrow (q \wedge \neg q)$

***PROPOSITION***: $\sqrt{2}$ is irrational.

***PROOF***: Assume $\sqrt{2}$ is NOT irrational, i.e., $\sqrt{2}$ is rational.
Then, there exist two integers *a* and *b* such that $\sqrt{2}=a/b$
and *a* and *b* are NOT both even.
Therefore, ......
......
In other words, $a^2$ is even.
Therefore, *a* is even.
However .....
......
Therefore, *a* and *b* are both even.
*contradiction*
Since our assumption leads to a contradiction, it must be false.
In other words, $\sqrt{2}$ IS irrational.



CIS1910 Proof Methods

## COMMON METHODS: Proofs by Cases 4.16

Based on the fact that $(p_1 \vee p_2) \rightarrow q \equiv (p_1 \rightarrow q) \wedge (p_2 \rightarrow q)$
A ***proof by cases*** of $(p_1 \vee p_2) \rightarrow q$ is a proof of $p_1 \rightarrow q$ and $p_2 \rightarrow q$

***PROPOSITION***: If n is an integer then $n^2 \geq n$.

***PROOF***: Assume n is an integer.
Then, n is negative, or n is zero, or n is positive.
*Case (i).* Let us prove that if n is a negative integer then $n^2 \geq n$.
......
*Case (ii).* Let us prove that if n is zero then $n^2 \geq n$.
......
*Case (iii).* Let us prove that if n is a positive integer then $n^2 \geq n$.
......

## COMMON METHODS: Existence Proofs 4.17

An ***existence proof*** is a proof of a proposition of the form $\exists x, P(x)$

---

***Constructive proof***: finding an element *a* such that P(*a*) is true.

***PROPOSITION***: There exists a positive integer that can be written as the sum of two cubes in two different ways.

***PROOF***: $1729 = 10^3+9^3 = 12^3+1^3$

---

***Nonconstructive proof***: proving that $\exists x, P(x)$ is true in some other way (e.g., proof by contradiction).

***PROPOSITION***: There exist irrationals x and y such that $x^y$ is rational.

***PROOF***: We know that $\sqrt{2}$ is irrational.
If $\sqrt{2}^{\sqrt{2}}$ is rational, we can pick $x=\sqrt{2}$ and $y=\sqrt{2}$.
If not, we can pick $x= \sqrt{2}^{\sqrt{2}}$ and $y=\sqrt{2}$ (since $x^y=2$).





## COMMON METHODS: Uniqueness Proofs 4.18

A ***uniqueness proof*** is a proof of a proposition of the form $\exists x, (P(x) \land \forall y, (y\neq x \rightarrow \neg P(y)))$
or $\exists x, (P(x) \land \forall y, (P(y) \rightarrow y=x))$

***PROPOSITION***: Let $(B,+,\cdot,\overline{\ })$ be a Boolean algebra.
There exists an element e of *B*, and only one, such that x+e=e for all x in *B*.

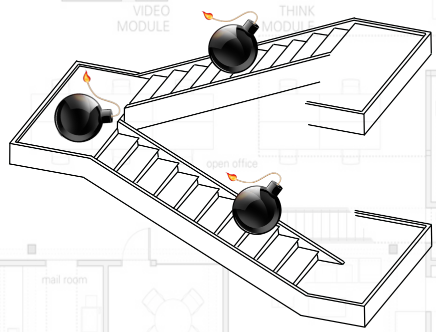
***PROOF***: *Existence.*
There exists an element e of *B* such that x+e=e for all x in *B*: the neutral element for · (domination law).

*Uniqueness.*
Let f be an element of *B* such that x+f=f for all x in *B*.
We have f+e=e (by definition of e; choose x=f).
However, we also have f+e=e+f (commutative law)
=f (by definition of f; choose x=e).
Therefore, e=f.

terminology
rules of inference
common proof methods
**PROOFS BY INDUCTION**

## PROOFS BY INDUCTION: Principle 4.21

**ASSUME THAT:**



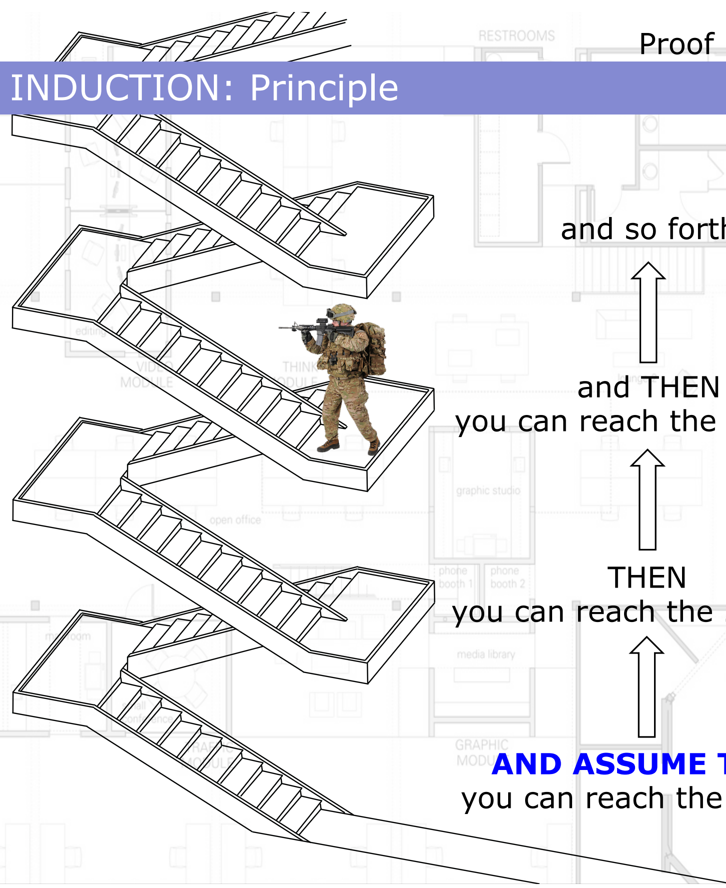
THEN
you can reach the floor n+1

⇧

IF
you can reach the floor n



## PROOFS BY INDUCTION: Principle 4.22



and so forth

⇧

and THEN
you can reach the 3rd floor

⇧

THEN
you can reach the 2nd floor

⇧

**AND ASSUME THAT:**
you can reach the 1st floor

## PROOFS BY INDUCTION: Examples (1/3) 4.23

Based on the rule of inference:
where the domain of P is 1..+∞

$$\frac{P(1) \quad \forall n, (P(n) \rightarrow P(n+1))}{\therefore \forall n, P(n)}$$

***PROPOSITION***: ∀n∈1..+∞, 1+2+…+n = n(n+1)/2

***PROOF***: Let P be the unary predicate whose domain is 1..+∞ and such that P(n) is the statement "1+2+…+n = n(n+1)/2".

P(1) is true, because 1=1(1+1)/2. ***basis step***

Let n be an arbitrary element of 1..+∞. Assume P(n) is true. ***inductive hypothesis***
Then, …… Therefore, ……
…..
In other words, P(n+1) is true. ***inductive step***

By induction, we can conclude that ∀n, P(n) is true.





## PROOFS BY INDUCTION: Examples (2/3) 4.24

Based on the rule of inference:
where the domain of P is 1..+∞

$$\frac{P(1) \quad \forall n, (P(n) \rightarrow P(n+1))}{\therefore \forall n, P(n)}$$

***PROPOSITION***: ∀n∈1..+∞, $\mathbf{6^{n+2}+7^{2n+1} \bmod 43 = 0}$

***PROOF***: Let P be the unary predicate whose domain is 1..+∞ and such that P(n) is the statement "$\mathbf{6^{n+2}+7^{2n+1} \bmod 43 = 0}$".

P(1) is true, because $\mathbf{6^3+7^3=559=43\times 13}$. *basis step*

Let n be an arbitrary element of 1..+∞. Assume P(n) is true. *inductive hypothesis*
Then, **……** Therefore, **……**
**…..**
In other words, P(n+1) is true. *inductive step*

By induction, we can conclude that ∀n, P(n) is true.

## PROOFS BY INDUCTION: Examples (3/3) 4.25

Based on the rule of inference: where the domain of P is **1**..+∞

P(**1**)
∀n, (P(n)→P(n+1))
∴ ∀n, P(n)

***could be any integer***

***PROPOSITION***: ∀n∈**0**..+∞, $6^{n+2}+7^{2n+1}$ mod 43 = 0

***PROOF***: Let P be the unary predicate whose domain is **0**..+∞ and such that P(n) is the statement "$6^{n+2}+7^{2n+1}$ mod 43 = 0".

P(**0**) is true, because $\mathbf{6^2+7^1=43}$.

Let n be an arbitrary element of **0**..+∞. Assume P(n) is true.
Then, ...... Therefore, ......
.....
In other words, P(n+1) is true.
By induction, we can conclude that ∀n, P(n) is true.





## PROOFS BY INDUCTION: How to Choose P (1/3) 4.26

**weak induction:** P(n)

***PROPOSITION***: For any n of 1..+∞,
1+2+…+n = n(n+1)/2

**strong induction:** P(n)

***PROPOSITION***: For any n of 1..+∞,
for any k of 1..+∞ such that k≤n,
1+2+…+k = k(k+1)/2

Q(k)

P(n) is of the form ∀k≤n, Q(k)

*inductive step*

Let n be an arbitrary element of 1..+∞. Assume P(n) is true.
Let us show that P(n+1) is true., i.e.,
let us show that 1+2+…+(n+1) = (n+1)(n+2)/2.
......

## PROOFS BY INDUCTION: How to Choose P (2/3) 4.27

**weak induction:** P(n)

***PROPOSITION***: For any n of 0..+∞, $6^{n+2}+7^{2n+1}$ mod 43 = 0

**strong induction:** P(n)

***PROPOSITION***: For any n of 0..+∞, for any k of 0..+∞ such that k≤n, $6^{k+2}+7^{2k+1}$ mod 43 = 0

P(n) is of the form ∀k≤n, Q(k)

Q(k): $6^{k+2}+7^{2k+1}$ mod 43 = 0

*inductive step*

Let n be an arbitrary element of 1..+∞. Assume P(n) is true.
Let us show that P(n+1) is true., i.e.,
let us show that $6^{(n+1)+2}+7^{2(n+1)+1}$ mod 43 = 0.
......





## PROOFS BY INDUCTION: How to Choose P (3/3) 4.28

**weak induction:** P(n)

***PROPOSITION***: For any n of 2..+∞, n is the product of primes

**strong induction:** P(n)

***PROPOSITION***: For any n of 2..+∞, for any k of 2..+∞ such that k≤n, k is the product of primes

P(n) is of the form ∀k≤n, Q(k)

Q(k): k is the product of primes

*inductive step*

Let n be an arbitrary element of 2..+∞. Assume P(n) is true.
Let us show that P(n+1) is true., i.e.,
let us show that n+1 is the product of primes.
......

terminology
rules of inference
common proof methods
proofs by induction

END