ANNOUNCEMENTS

- Homework 3 is out on Canvas:
  - Due date: May 25 (midnight) on Canvas
    - Should be submitted as a pdf file
- Quiz 6: May 14, last 10 minutes of class.
  - Material: "Entracte" chapter from Logicomix and lectures on 5/7 and 5/12
- Exam 2: June 2. Canvas quiz during class time. Covering all month of May.

ZYBOOK MATERIAL

- Today we will finish with logic
  - 2.12 (valid arguments in English-part of homework)
  - and 2.13 (Rules of inference with quantifiers)

- And then jump into "Proofs"
  - Chapter 4 of ZyBooks

- First: Equivalence between Section 2.12 in ZyBooks and the Hillbert system of the Cheat Sheet

Rule of inference	Name
p $p \to q$ $\therefore q$	Modus ponens
$\neg q$ $p \to q$ $\therefore \neg p$	Modus tollens
p $\therefore p \vee q$	Addition
$p \wedge q$ $\therefore p$	Simplification
p q $\therefore p \wedge q$	Conjunction
$p \to q$ $q \to r$ $\therefore p \to r$	Hypothetical syllogism
$p \vee q$ $\neg p$ $\therefore q$	Disjunctive syllogism
$p \vee q$ $\neg p \vee r$ $\therefore q \vee r$	Resolution

- Modus Ponens
  - $p, p \to q \vdash q$

Theorem 6 $\alpha \to \beta, \neg\beta \vdash \neg\alpha$

Rule 7 $\alpha \vdash \alpha \vee \beta$

Rule 8 $\beta \vdash \alpha \vee \beta$

Rule 4 $\alpha \wedge \beta \vdash \alpha$

Rule 5 $\alpha \wedge \beta \vdash \beta$

Theorem 10 $\alpha, \beta \vdash \alpha \wedge \beta$

Theorem 2 $\alpha \to \beta, \beta \to \gamma \vdash \alpha \to \gamma$

Theorem 11 $\alpha \vee \beta, \neg\alpha \vdash \beta$

Not in cheat sheet, but easily provable

VALID ARGUMENTS

- With these hypotheses:
  "It is not sunny this afternoon 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."
- Using the inference rules, construct a valid argument for the conclusion:
  "We will be home by sunset."

Solution:

1. Choose propositional variables:
   p : "It is sunny this afternoon." r : "We will go swimming."
   t : "We will be home by sunset."
   q : "It is colder than yesterday." s : "We will take a canoe trip."
2. Translation into propositional logic:

$$\text{Hypotheses: } \neg p \wedge q,\ r \rightarrow p,\ \neg r \rightarrow s,\ s \rightarrow t$$
$$\text{Conclusion: } t$$

Continued on next slide →

VALID ARGUMENTS

3. Construct the Valid Argument

Step	Reason
1. $\neg p \wedge q$	Premise
2. $\neg p$	Simplification using (1)
3. $r \rightarrow p$	Premise
4. $\neg r$	Modus tollens using (2) and (3)
5. $\neg r \rightarrow s$	Premise
6. s	Modus ponens using (4) and (5)
7. $s \rightarrow t$	Premise
8. t	Modus ponens using (6) and (7)

HANDLING QUANTIFIED STATEMENTS

- Valid arguments for quantified statements are a sequence of statements. Each statement is either a premise or follows from previous statements by rules of inference which include:
  - Rules of Inference for Propositional Logic
  - Rules of Inference for Quantified Statements
- The rules of inference for quantified statements are introduced in the next several slides.

UNIVERSAL INSTANTIATION (UI)

$$\frac{\forall x P(x)}{\therefore P(c)}$$

Example:

Our domain consists of all dogs and Fido is a dog.

"All dogs are cuddly."

"Therefore, Fido is cuddly."

UNIVERSAL GENERALIZATION (UG)

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

Used often implicitly in Mathematical Proofs.

EXISTENTIAL INSTANTIATION (EI)

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

Example:

"There is someone who got an A in the course."
"Let's call her *a* and say that *a* got an A"

EXISTENTIAL GENERALIZATION (EG)

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

Example:

"Michelle got an A in the class."
"Therefore, someone got an A in the class."

SUMMARY

Table 2.13.1: Rules of inference for quantified statements.

Rule of Inference	Name	Example
c is an element (arbitrary or particular) $\forall x\ P(x)$ $\therefore P(c)$	Universal instantiation	Sam is a student in the class. Every student in the class completed the assignment. Therefore, Sam completed his assignment.
c is an arbitrary element $P(c)$ $\therefore \forall x\ P(x)$	Universal generalization	Let c be an arbitrary integer. $c \leq c^2$ Therefore, every integer is less than or equal to its square.
$\exists x\ P(x)$ $\therefore$ (c is a particular element) $\wedge$ P(c)	Existential instantiation*	There is an integer that is equal to its square. Therefore, $c^2 = c$, for some integer c.
c is an element (arbitrary or particular) $P(c)$ $\therefore \exists x\ P(x)$	Existential generalization	Sam is a particular student in the class. Sam completed the assignment. Therefore, there is a student in the class who completed the assignment.

*Note: each use of Existential instantiation must define a new element with its own name (e.g., "c" or "d").

ZyBook 2.13.2

USING RULES OF INFERENCE

Example 1: Using the rules of inference, construct a valid argument to show that

"John Smith has two legs"

is a consequence of the premises:

"Every man has two legs." "John Smith is a man."

Solution: Let $M(x)$ denote "x is a man" and $L(x)$ " x has two legs" and let John Smith be a member of the domain.

Valid Argument:

Step	**Reason**
1. $\forall x(M(x) \rightarrow L(x))$	Premise
2. $M(J) \rightarrow L(J)$	UI from (1)
3. $M(J)$	Premise
4. $L(J)$	Modus Ponens using (2) and (3)

USING RULES OF INFERENCE

Example 2: Use the rules of inference to construct a valid argument showing that the conclusion

"Someone who passed the first exam has not read the book."

follows from the premises

"A student in this class has not read the book."

"Everyone in this class passed the first exam."

Solution: Let $C(x)$ denote "x is in this class," $B(x)$ denote "x has read the book," and $P(x)$ denote "x passed the first exam."

First we translate the premises and conclusion into symbolic form.

$$\begin{array}{l} \exists x(C(x) \wedge \neg B(x)) \\ \forall x(C(x) \rightarrow P(x)) \\ \hline \therefore\ \exists x(P(x) \wedge \neg B(x)) \end{array}$$

Continued on next slide →

USING RULES OF INFERENCE

Valid Argument:

Step	**Reason**
1. $\exists x(C(x) \wedge \neg B(x))$	Premise
2. $C(a) \wedge \neg B(a)$	EI from (1)
3. $C(a)$	Simplification from (2)
4. $\forall x(C(x) \rightarrow P(x))$	Premise
5. $C(a) \rightarrow P(a)$	UI from (4)
6. $P(a)$	MP from (3) and (5)
7. $\neg B(a)$	Simplification from (2)
8. $P(a) \wedge \neg B(a)$	Conj from (6) and (7)
9. $\exists x(P(x) \wedge \neg B(x))$	EG from (8)

RETURNING TO THE SOCRATES EXAMPLE

$$\forall x(Man(x) \rightarrow Mortal(x))$$

$$Man(Socrates)$$

$$\therefore \quad Mortal(Socrates)$$

SOLUTION FOR SOCRATES EXAMPLE

Valid Argument

Step	**Reason**
1. $\forall x(Man(x) \rightarrow Mortal(x))$	Premise
2. $Man(Socrates) \rightarrow Mortal(Socrates)$	UI from (1)
3. $Man(Socrates)$	Premise
4. $Mortal(Socrates)$	MP from (2) and (3)

INTRODUCTION TO PROOFS

DEFINITIONS

- A *theorem* is a statement that can be shown to be true using:
  - definitions
  - other theorems
  - *axioms* (statements which are given as true)
  - rules of inference
- A *lemma* is a 'helping theorem' or a result which is needed to prove a theorem.
- A *corollary* is a result which follows directly from a theorem.
- Less important theorems are sometimes called *propositions*.
- A *conjecture* is a statement that is being proposed to be true. Once a proof of a conjecture is found, it becomes a theorem. It may turn out to be false.

SECTION SUMMARY

- Mathematical Proofs
- Forms of Theorems
- Direct Proofs
- Indirect Proofs
  - Proof of the Contrapositive
  - Proof by Contradiction

PROOFS OF MATHEMATICAL STATEMENTS

- A *proof* is a valid argument that establishes the truth of a statement.
- Proofs have many practical applications:
  - verification that computer programs are correct
  - establishing that operating systems are secure (check out seL4)
  - enabling programs to make inferences in artificial intelligence
  - showing that system specifications are consistent
- In math, CS, and other disciplines, informal proofs which are generally shorter, are generally used.
  - More than one rule of inference are often used in a step.
  - Steps may be skipped.
  - The rules of inference used are not explicitly stated.
  - Easier for to understand and to explain to people.
  - But it is also easier to introduce errors.

WHAT IS WRONG WITH THIS?

If a = b then *1 = 2*

Step	**Reason**
1. $a = b$	Premise
2. $a^2 = a \times b$	Multiply both sides of (1) by a
3. $a^2 - b^2 = a \times b - b^2$	Subtract b^2 from both sides of (2)
4. $(a - b)(a + b) = b(a - b)$	Algebra on (3)
5. $a + b = b$	Divide both sides by $a - b$
6. $2b = b$	Replace a by b in (5) because $a = b$
7. $2 = 1$	Divide both sides of (6) by b

Solution: Step 5. a - b = 0 by the premise and division by 0 is undefined.

FORMS OF THEOREMS

- Many theorems assert that a property holds for all elements in a domain, such as the integers, the real numbers, or some of the discrete structures that we will study in this class.
- Often the universal quantifier (needed for a precise statement of a theorem) is omitted by standard mathematical convention.

For example, the statement:

"If $x > y$, where x and y are positive real numbers, then $x^2 > y^2$ "

really means

"For all positive real numbers x and y, if $x > y$, then $x^2 > y^2$."

SOME EASY PROOFS

- Counterexamples
- Existence proofs
- Trivial proofs
- Vacuous proofs

COUNTEREXAMPLES

- Recall $\exists x \neg P(x) \equiv \neg \forall x P(x)$
- To establish that $\neg \forall x P(x)$ is true (or $\forall x P(x)$ is false) find a *c* such that $\neg P(c)$ is true or $P(c)$ is false.
- In this case *c* is called a *counterexample* to the assertion

$$\forall x P(x)$$

Example: "Every positive integer is the sum of the squares of 3 integers." The integer 7 is a counterexample. So the claim is false.

EXISTENCE PROOFS

- Proof of theorems of the form $\exists x P(x)$
- **Constructive** existence proof:
  - Find an explicit value of *c*, for which *P(c)* is true.
  - Then $\exists x P(x)$ is true by Existential Generalization (EG).

Example: Show that there is a positive integer that can be written as the sum of cubes of positive integers in two different ways:

Proof: 1729 is such a number since

$$1729 = 10^3 + 9^3 = 12^3 + 1^3$$

◀

UNIQUENESS PROOFS = EXISTENCE + UNIQUENESS

- Some theorems asset the existence of a unique element with a particular property, $\exists! x\, P(x)$. The two parts of a *uniqueness proof* are
  - *Existence*: We show that an element x with the property exists.
  - *Uniqueness*: We show that if $y \neq x$, then y does not have the property.

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: The real number $r = -b/a$ is a solution of $ar + b = 0$ because $a(-b/a) + b = -b + b = 0$.
- Uniqueness: Suppose that s is a real number such that $as + b = 0$. Then $ar + b = as + b$, where $r = -b/a$. Subtracting b from both sides and dividing by a shows that $r = s$.

◀

PROVING THEOREMS

- Many theorems have the form: $\forall x(P(x) \rightarrow Q(x))$
- To prove them, we show that where *c* is an arbitrary element of the domain, $P(c) \rightarrow Q(c)$
- By universal generalization the truth of the original formula follows.
- So, we must prove something of the form: $p \rightarrow q$

PROVING CONDITIONAL STATEMENTS: $P \rightarrow Q$

- *Trivial Proof*: If we know q is true, then

  $p \rightarrow q$ is true as well.

"If it is raining then $1=1$."

- *Vacuous Proof*: If we know p is false then

  $p \rightarrow q$ is true as well.

"If I am both rich and poor then $2 + 2 = 5$."

[Even though these examples seem silly, both trivial and vacuous proofs are often used in mathematical induction)]

MORE GENERAL PROOFS

- Direct proofs
  - But first we need definitions

DEFINITIONS

Definition 4.1.1: Even and odd integers.

An integer x is ***even*** if there is an integer k such that x = 2k.
An integer x is ***odd*** if there is an integer k such that x = 2k+1.

Definition 4.1.2: The real number *r* is *rational* if there exist integers *p* and *q* where $q \neq 0$ such that $r = p/q$

Definition 4.1.3: Divides.

An integer x ***divides*** an integer y if and only if y = kx, for some integer k.

The fact that x divides y is denoted x|y. If x does not divide y, then that fact is denoted x∤y.

If x divides y, then y is said to be a ***multiple*** of x, and x is a ***factor*** or ***divisor*** of y.

Definition 4.1.4: Prime and composite numbers.

An integer n is ***prime*** if and only if n > 1, and for every positive integer m, if m divides n, then m = 1 or m = n.

An integer n is ***composite*** if and only if n > 1, and there is an integer m such that 1 < m < n and m divides n.

ZyBook 4.1 exercises

ALLOWED ASSUMPTIONS IN PROOFS

The rules of algebra.

For example if x, y, and z are real numbers and $x = y$, then $x+z = y+z$.

The set of integers is closed under addition, multiplication, and subtraction.

In other words, sums, products, and differences of integers are also integers.

Every integer is either even or odd.

This fact is proven elsewhere in the material.

If x is an integer, there is no integer between x and x+1.

In particular, there is no integer between 0 and 1.

The relative order of any two real numbers.

For example $1/2 < 1$ or $4.2 \geq 3.7$.

The square of any real number is greater than or equal to 0.

This fact is proven in a later exercise.

PROVING CONDITIONAL STATEMENTS: $P \rightarrow Q$

- *Direct Proof*: Assume that p is true. Use rules of inference, axioms, and logical equivalences to show that q must also be true.

Theorem: If n is an odd integer, then n^2 is odd.

Solution: Assume that n is odd. Then $n = 2k + 1$ for an integer k. Squaring both sides of the equation, we get:

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 = 2r + 1,$$

where $r = 2k^2 + 2k$, an integer.

(integers are closed under multiplication)

We have proved that if n is an odd integer, then n^2 is an odd integer.

◄

(◄ marks the end of the proof. Sometimes **QED** is used instead.)