

# CS3512, Fall 2011

**Instructor:** Hudson Turner

**Textbook:** James L. Hein, *Discrete Structures, Logic, and Computability*, 3rd Ed. Jones and Barlett, 2010.

Prerequisites: Calc I, CS II

This is a required course for CS majors. Why?

- ▶ Standard material on discrete math.
- ▶ Intro to mathematical foundations of computation.
- ▶ Necessary for an accredited CS program.

This is a demanding course. Why?

- ▶ Some of the definitions are subtle and have surprising ramifications.
- ▶ Emphasis on proofs!

Why study proofs?

- ▶ Proof is a wonderful method for deep understanding.
- ▶ We can only study a sample of topics in discrete math and theoretical CS — work on proofs prepares you to study further on your own.
- ▶ Habits of thought necessary for writing or understanding proofs can be useful in much of CS.

# Rough course outline

We cover a selection of material from Ch 1–5, 11 of the textbook.

(As the course progresses, our treatment diverges further and further from the book's.)

- ▶ *Proofs!*
- ▶ Sets, tuples, lists, strings, relations, trees
- ▶ Functions, countability, diagonalization
- ▶ Inductively defined sets, recursive functions
- ▶ Structural and mathematical induction
- ▶ Program correctness (prove correctness of recursive programs by induction)
- ▶ Time/space analysis of algorithms (big O)
- ▶ Regular expressions, finite automata

## Course organization

### Details in syllabus

No graded homework, but you should expect to work lots of problems on your own outside of class. . .

You learn math by *doing* math!

Ask questions!!

Quiz most Tuesdays (10 pts each, drop lowest 2)

Pop quizzes (5 pts each, drop lowest 2)

Three 75 minute exams during semester (75 points each), plus scheduled final (125 points)

Grades based on total points (strong curve)

Why no graded homework? Why so much time devoted to quizzes?

- ▶ I know who does what on quizzes — more fair as a basis for grading.
- ▶ All students do quiz problems at same time. We can discuss soon after — fresh in everyone's mind.
- ▶ I grade quizzes personally — try do it quickly, carefully, giving detailed feedback.
- ▶ Frequent quizzes encourage frequent study outside of class.

Some of the quiz problems will be hard — please don't be discouraged by this.

Trying to develop solid reliance on definitions, and clear expression of mathematically sound reasoning.

## Logical form of statements

We consider statements that are either true or false.

### Negation

If

$S$

is a statement, its *negation* is the statement

not  $S$ .

[Consider truth table for negation]

We often rephrase:

“Earth is not a star” instead of “Not Earth is a star”.

### Quantifiers: every and some

Nicely related via negation: “Not every planet has a moon” has the same meaning as “some planet doesn't have a moon”. Similarly, “no planet is a star” has the same meaning as ...

## Conjunction and disjunction

The *conjunction* of statements  $A$  and  $B$  is the statement

$A$  and  $B$ .

It is true when both  $A$  and  $B$  are.

The *disjunction* of statements  $A$  and  $B$  is the statement

$A$  or  $B$ .

It is true when at least one of  $A$  and  $B$  is.

[Consider truth table for conjunction and disjunction]

Sometimes rephrased:

“Earth and Mars are planets” instead of ...

“Either  $x$  or  $y$  is positive” instead of ...

## Conditionals

If  $A$  and  $B$  are statements, then

if  $A$  then  $B$

is a *conditional* statement whose *hypothesis* is  $A$  and whose *conclusion* is  $B$ .

A conditional is false only when the hypothesis is true and the conclusion is false.

[Consider truth table for conditional]

You may need to be careful about this one – not necessarily a “causal” connection between hypothesis and conclusion.

The *converse* of

if  $A$  then  $B$

is the statement

if  $B$  then  $A$ .

Notice that a conditional and its converse may have different truth values.

If  $x$  and  $y$  exceed 0, then so does  $x + y$ .

## Equivalent statements

“not (not  $A$ )” is equivalent to “ $A$ ”

“not ( $A$  and  $B$ )” is equivalent to “(not  $A$ ) or (not  $B$ )”

“not ( $A$  or  $B$ )” is equivalent to ...

Example: Simplify “not ( $x > 0$  and  $y > 0$ )”

$A$  and ( $B$  or  $C$ )  $\Leftrightarrow$  ( $A$  and  $B$ ) or ( $A$  and  $C$ )

$A$  or ( $B$  and  $C$ )  $\Leftrightarrow$  ...

The *contrapositive* of a conditional statement

if  $A$  then  $B$

is the equivalent statement

if not  $B$  then not  $A$ .

if  $A$  then  $B$   $\Leftrightarrow$  (not  $A$ ) or  $B$

not (if  $A$  then  $B$ )  $\Leftrightarrow$  ...

## Overview of proof techniques

### Proof by exhaustive checking

May be useful when a statement asserts that each of a **finite** number of things has a property.

May not be practical if there are many of these things.

Not applicable if there are infinitely many things.

### Proof by counterexample

We can often prove the falsity of a (false) universal claim by finding an instance that falsifies it.

Example: “Every odd number greater than 1 that is not prime has the form  $2 + p$  for some prime number  $p$ .” (What is a counterexample?)

### **Direct conditional proof**

To prove “if  $A$  then  $B$ ”, assume  $A$  in order to derive  $B$ .

### **Indirect conditional proof, or proof by contrapositive**

To prove “if  $A$  then  $B$ ”, assume the negation of  $B$  in order to derive the negation of  $A$ .

### **Indirect proof by contradiction**

To prove  $A$ , assume the negation of  $A$  and derive a contradiction.

How would this work if you wished to prove “if  $A$  then  $B$ ” by contradiction?

### **Iff proof in two parts**

“ $A$  iff  $B$ ” stands for “ $A$  if and only if  $B$ ”, which in turn stands for “(if  $A$  then  $B$ ) and (if  $B$  then  $A$ )”.

[What is the truth table for iff?]

A typical approach to proving an iff claim is to prove the two conditionals separately. (“left-to-right” and “right-to-left”)

### **Iff proof by chain of equivalences**

An alternative approach is to find a chain of iff claims that takes you from  $A$  to  $B$ .

### **Constructive proof of existence**

If a statement asserts that an object with some property exists, there are typically two approaches: either use proof by contradiction or construct an instance with the property. The second, “constructive” approach is usually preferable.

## General remarks on proofs

Write out your proofs carefully. (Or proofread and edit them well.)

Have a plan, and present your proof so that the reader can follow the plan.

Say enough to make your reasoning clear.

Be clear about where variables come from. (This will become clearer.)

Use definitions as they are. (Don't use intuitions as facts.)

About finding proofs...

Try various proof structures, based on the structure of the claim!

Apply **definitions**.

If you're stuck, maybe it will help to consider cases.

Look at instances of the claim you're trying to prove. (For "intuition"!) )

Do something else, and come back to it later.

Review examples in textbook and lecture.

## Integers, divisibility, primality: something to talk about

The integers:

$$\dots, -3, -2, -1, 0, 1, 2, 3, \dots$$

An *even* integer can be written  $2n$  for some integer  $n$ .

An *odd* integer can be written  $2n + 1$  for some integer  $n$ .

An integer  $d$  *divides* an integer  $n$  if  $d \neq 0$  and there is an integer  $k$  such that

$$n = dk.$$

We write

$$d \mid n$$

to say that  $d$  divides  $n$ .

( " $d$  is a factor, or divisor, of  $n$ ", " $n$  is divisible by  $d$ ", ... )

Notice: It follows easily that the even integers are the integers  $n$  such that  $2 \mid n$ .

An integer  $p > 1$  is *prime* if 1 and  $p$  are its only positive divisors.

## Proof examples

**Claim:** The sum of any two odd integers is an even integer.

**Proof outline:**

1. Rephrase as a universally quantified conditional.

**For all** integers  $x, y$ ,  
**if**  $x$  and  $y$  are odd, **then**  $x + y$  is even.

2. Instantiate the universally quantified variables.

Take arbitrary integers  $x, y$ .

3. Assume the hypothesis (direct conditional proof).

Assume that  $x$  and  $y$  are odd.

4. Apply the relevant definition.

5. Derive the conclusion (of the conditional).

**Claim:** The sum of any two odd integers is an even integer.

**Proof** Take arbitrary integers  $x, y$ . Assume that  $x$  and  $y$  are odd.

We need to show that  $x + y$  is even.

Since  $x$  and  $y$  are odd, there are integers  $m, n$  s.t.

$$x = 2m + 1 \quad \text{and} \quad y = 2n + 1.$$

Notice that

$$\begin{aligned} x + y &= 2m + 1 + 2n + 1 \\ &= 2(m + n + 1) \end{aligned}$$

Since  $m + n + 1$  is an integer, we can conclude that  $x + y$  is even. (Why?)

[Something a bit subtle happened here: We observed that since  $x$  is odd, it follows (by the defn of odd) that there exists an integer  $m$  s.t.  $x = 2m + 1$ . That's straightforward. The subtle part is that, from then on, when we wrote  $m$ , we meant the reader to understand that  $m$  is an instance of just such an integer. Of course the same story can be told about the use of  $n$  above. These variable names were introduced via a claim, or deduction, about the existence of a certain object. This is very convenient, and we'll do it alot.]

Let's do it again, more like we'll normally do it. . .

**Claim:** The sum of any two odd integers is an even integer.

**Proof** Assume that  $x$  and  $y$  are odd integers. [NTS:  $x + y$  is even]

So there are integers  $m, n$  s.t.

$$x = 2m + 1 \quad \text{and} \quad y = 2n + 1.$$

Notice that

$$\begin{aligned} x + y &= 2m + 1 + 2n + 1 \\ &= 2(m + n + 1) \end{aligned}$$

Since  $m + n + 1$  is an integer, it follows that  $x + y$  is even.

Claim: If  $d \mid a$  and  $a \mid b$ , then  $d \mid b$ . (1.1a)

Again let's try a direct conditional proof. . .

Claim: If  $x^2$  is odd, then  $x$  is odd.

Let's try an indirect proof by contrapositive...

[Useful lemma: For all integers  $n$ ,  $n$  is even iff  $n$  is not odd. (Your textbook uses this lemma without seeming to notice. Can you prove it?)]

Claim: If  $n$  is an integer, then  $n^2 + 2$  is not divisible by 4.

We'll use proof by contradiction.

(Within this, consider cases on whether or not  $n$  is even.)

Proof: Suppose that  $n$  is an integer s.t.  $n^2 + 2$  is divisible by 4. (What is our goal now?)

That is,  $4 \mid (n^2 + 2)$ , which implies that

$$n^2 + 2 = 4k \tag{1}$$

for some integer  $k$ .

Consider two cases. (What will we derive in each case?)

Case 1:  $n$  is even. That is,  $n = 2m$  for some integer  $m$ . Then

$$\begin{aligned} 4k &= n^2 + 2 && \text{(by (1))} \\ &= (2m)^2 + 2 && (n = 2m) \\ &= 4m^2 + 2 \end{aligned}$$

Dividing by 2, we have  $2k = 2m^2 + 1$ . The lhs is even; the rhs is odd.

Contradiction (by the earlier lemma, if the rhs is odd we know it is *not* even).

Case 2:  $n$  is not even. [Try this. Similar to case 1.]

Claim: Every integer greater than 1 is divisible by a prime.

Proof by contradiction.

[Try it. Tough one. Textbook has a proof. Try to understand it and present it more clearly.]

For the following example, we'll want several lemmas:

1. For any integer  $n$ ,  $n(n + 1)$  is even.
2. Exactly one of any two consecutive integers is even.
3. No even number divides an odd number.

[You should try to prove these yourself.]

Claim:  $x$  is odd iff  $8 \mid (x^2 - 1)$ .

Try proving both directions.

Proof: (Left-to-right) Assume that  $x$  is odd. That is,  $x = 2k + 1$  for some integer  $k$ . So

$$x^2 - 1 = (2k + 1)^2 - 1 = 4k^2 + 4k = 4k(k + 1).$$

Since  $k$  and  $k + 1$  are consecutive integers, their product is even (by lemma 1 above), so  $k(k + 1) = 2m$  for some integer  $m$ . Substituting for  $k(k + 1)$  above, we have

$$x^2 - 1 = 4(2m) = 8m,$$

which shows that 8 divides  $x^2 - 1$ .

(Right-to-left) Assume  $x$  is not odd. (What is our goal now!?) By previous lemma, it follows that  $x$  is even. Since  $x$  is even, we know  $x^2$  is even (by earlier claim), and so (by lemma 2 above)  $x^2 - 1$  is odd. By lemma 3 above, no even number divides an odd number. So 8 does not divide  $x^2 - 1$ .

Claim:  $x$  is odd iff  $x^2 + 2x + 1$  is even.

Proof by chain of equivalences.

For this proof, we'll want the following easy lemma.

Lemma.  $x$  is even iff  $x^2$  is even. (Try to prove it.)

Proof of claim:

$x$ is odd	iff	$x = 2k + 1$ for some integer $k$	(defn odd)
	iff	$x + 1 = 2(k + 1)$ for some integer $k$	
	iff	$x + 1$ is even	(defn even)
	iff	$(x + 1)^2$ is even	(Lemma)
	iff	$x^2 + 2x + 1$ is even	

In the chain of iffs, we included the phrase "for some integer  $k$ " twice. . .

$x$ is odd	iff	$x = 2k + 1$ for some integer $k$	(defn odd)
	iff	$x + 1 = 2(k + 1)$ for some integer $k$	
	iff	$x + 1$ is even	(defn even)
	iff	$(x + 1)^2$ is even	(Lemma)
	iff	$x^2 + 2x + 1$ is even	

What happens if we drop both occurrences of "for some integer  $k$ "?

The argument is no longer sound.

For instance, is the claim in the first step still true? That is, do we believe that

$$x \text{ is odd iff } x = 2k + 1$$

Hint: Even if we assume that  $x$  and  $k$  are both integers, it is possible to falsify this claim.