



6.042/18.062J

Spring 2011

- [Courseinfo](#)
- [Outcomes](#)
- [Contact](#)
- [Statistics](#)
- [Class List†](#)

Course Overview

Contents

- [Introduction](#)
- [Considerations for Taking the Subject This Term](#)
- [Team Problem Solving](#)
- [Weekly Schedule](#)
- [Course Website](#)
- [Problem Sets](#)
- [Online Tutor Problems](#)
- [Weekly Reading Comments](#)
- [Biweekly Miniquizzes](#)
- [Collaboration](#)
- [Grades](#)
- [Email Forum](#)
- [Latex Macros](#)

Introduction

This subject offers an introduction to Discrete Mathematics oriented toward Computer Science and Engineering. It meets MWF in 26-152 (TEAL) 12:30–2:00PM. There are no separate recitations. The subject coverage divides into three parts:

1. Fundamental concepts of Mathematics: definitions, proofs, sets, functions, elementary number theory
2. Discrete structures: graphs, counting.
3. Discrete probability theory.

The prerequisite is 18.01 (first term calculus), in particular, some familiarity with sequences and series, limits, and differentiation and integration of functions of one variable.

The goals of the course are summarized in a statement of [Course Objectives and Educational Outcomes](#). A detailed schedule of topic coverage appears in the [Course Calendar](#).

Considerations for Taking the Subject This Term

There are two main considerations for students in deciding to take 6.042J/18.062J *this term*—or at all.

1. Team Problem Solving

This term, as in many previous terms, the subject is being taught in Lecture/Team Problem Solving style. More about two thirds of class meeting time will be devoted to problem solving in teams of 7–9 sitting around a table with a nearby whiteboard where a team can write their solutions. Each TA, assisted by an LA, covers 3 tables, acting as coach and providing feedback on students' solutions. The Lecturer acts likewise, circulating among all the tables. The coach will resist answering questions about the material, always trying first to find a team member who can explain the answer to the rest of the team. Of

course the coach will provide hints and explanations when the whole team is stuck.

Problem solving sessions will generally be preceded by half hour presentations by the lecturer, usually reviewing just the topics needed to understand the problems. These overviews are not intended as first-time introductions to the material nor as complete coverage of the assigned reading.

The Good News is that the immediate, active engagement in problem solving sessions is an effective and enjoyable way for most students to master the material. Team sessions also provide a supervised setting to acquire and practice technical communication skills. Student grades for problem solving sessions depend on degree of *active, prepared* participation, rather than problem solving success. Sessions are not aimed to test how well a student can solve the problems in class; the goal is to have them understand how to solve them by the end of the session. Participation in team sessions counts for 20% of the final grade.

In-class team problem solving works to solidify students' understanding of *material they have already seen*. The Bad News is that this requires students to arrive *prepared* at the sessions: they need to have read (though not carefully studied) the assigned reading and done the [Online Tutor](#) problems before class. There is no way to make up for not working with the team, so it is necessary to keep up and be there —no focusing on something else for a month, aiming to catch up afterward. **If you cannot commit to keeping up, you may prefer to take the subject some other term.**

2. This subject covers many of mathematical topics that are essential in Computer Science and are not covered in the standard calculus curriculum. In addition, the subject teaches students about careful mathematics: precisely stating assertions about well-defined mathematical objects and verifying these assertions using mathematically sound proofs. While some students have had earlier exposure to some of these topics, in most cases they learn a lot more in 6.042J/18.062J.

The subject is required of all Computer Science (6-3) majors and is in a required category for Math majors taking the Computer Science option (18C). But students with a firm understanding of sound proofs, and who are familiar with many of the covered topics, should discuss substituting a more advanced Math subject for 6.042 with the Lecturer or their advisor.

Weekly Schedule

- **Class Text**

Successive revised chapters of our own class textbook will be available weekly for download.

- **Online Tutor Problems & Reading Comments**

These are generally due at 9AM before class. See the [Online Tutor](#) and [reading comments](#) information below.

- **Problem Sets**

Problem sets will usually be due at the beginning of class Friday. They are assigned a week or more in advance. The exact schedule is posted the [Course Calendar](#). See [Problem Sets](#) below for further information.

- **Miniquizzes**

Miniquizzes are given every other week, usually on Wednesdays. See [Biweekly Miniquizzes](#) below for further information.

Course Website

The class has a comprehensive web site:

<http://courses.csail.mit.edu/6.042>

Notes, problem sets, solutions, etc., will be posted in the [course calendar](#). Other course information such as [staff contact information](#), [mailing lists](#), and [announcements](#) are also available on this website. It is **always worth checking the website** for corrections and announcements before starting problem sets.

Problem Sets

Problem Sets are normally due at the beginning of lecture on Fridays, but a few may be due at alternate times because of holidays. Doing the problem sets is, for most students, crucial for mastering the course material. Solutions to the problem sets will be posted immediately after the due date. Consequently, **late problem sets will not be accepted**.

Problem sets count for 25% of the final grade. To reduce problem sets as a source of pressure, and as a reflection of their intended teaching —as opposed to testing—purpose, students can make up half the credit for a pset on the subsequent miniquiz and on the final. But aiming only for half credit on problem sets with intention of making up the missing half credit on subsequent exams is a risky strategy, especially since grades on the final tend to be lower than on problem sets.

For example, if a student missed 4 points on a 10 point pset, then 2 of those missed points get added to the weight of the next miniquiz and 2 to the final exam. If a student missed more than half the points on a 10 point pset, then 5 points can be made up —2.5 of the missed points get added to the weight of the next miniquiz and 2.5 to the final exam.

Students are encouraged to [collaborate](#) on problem sets as on teams in class. The last page of each problem set has a **collaboration statement** to be completed and attached as the first page of a pset submission:

"I worked alone and only with course materials"

or

"I collaborated on this assignment with *<students in class>*, got help from *<people other than collaborators and course staff>*, and referred to *<citations to sources other than the class material from this term>*".

No problem set will be given credit until it has a collaboration statement.

Graders time is limited, and when in doubt about an unclear student solution, they are instructed initially to deny credit. If a student is concerned about how a pset has been graded, they should take it up with their LA or TA after class. If they're not satisfied with the TA's response, the Lecturer will be happy to hear an appeal.

Online Tutor Problems

There are weekly Online Tutor problems due before class on specified dates. These consist of straightforward questions that provide useful feedback about the assigned material. Tutor problems should take about 20 minutes after the reading has been completed. (Some students prefer to try the tutor problems before doing the reading, which is fine.)

Like team problem-solving in class, online tutor problems are graded solely on *participation*: students receive full credit as long as they try the problem, even if their answer is wrong. Tutor problems count for 5% of the final grade.

Weekly Reading Comments

A comment in email to 6042-probs@csail.mit.edu on the week's reading is due on specified dates by 9AM before class. (This email address may not be activated until Monday, Feb. 7.)

As single comment citing some paragraph that specially catches your is all that is required. The comment should indicate why this paragraph stood out, for example, because you found it especially

- difficult/confusing, or
- surprising, or
- mistaken (pointing out typos & suggesting corrections is appreciated), or
- funny, or
- boring, or
- lacking Computer Science motivation, or
- poorly written,
- something you'd like reviewed in class,

Multiple comments are welcomed.

Note that global comments such as *"I understood everything in the reading, found it all (un?)interesting, and have no questions"* are not considered responsive. Even if you understood everything, there must, in the 15 to 30 pages assigned each week, have been something that stood out for you as suggested above.

Reading comments count for 3% of the final grade.

Collaboration and Outside Sources

We encourage students to **collaborate on homework** as on in-class problems. Study groups can be a big help in mastering course material, besides being fun and a good way to make friends. However, students must **write up solutions on their own**, neither copying solutions nor providing solutions to be copied. All collaborators must **cited**, and if a source beyond the course materials is used in a solution—for example, an "expert" consultant other than 6.042 staff, or another text—there must be a **proper scholarly citation of the source**.

Subject materials for Spring '10 are available on OCW; solutions for psets and final exams are not included however. Complete material including solutions are available if OCW for Fall '05 and Spring '05. The material this term will be similar to that of the Spring '10, though in a different order largely following the Fall '10 text. A problem from these prior terms may occasionally be assigned again without change. If a student looks at the published solution, they should **cite it, and may not simply copy the published solution**. Instead, a critique of the published solution or an improved version should be submitted instead.

We discourage, but do not forbid, use of materials from prior terms other than available on OCW. We repeat, however, that use of material from any previous term requires a **proper scholarly citation**. As long as a student provides accurate citation and collaboration statements, a questionable submission will rarely be sanctioned—instead, we'll explain why we judge the submission unsatisfactory (and maybe deny credit for specific, clearly copied solutions). But *omission* of such a citation will be taken as a *priori* evidence of cheating, with unpleasant consequences for everyone.

Biweekly Miniquizzes

A 25–30 minute Miniquiz will generally be given every other week, usually on Wednesdays. Miniquizzes count for a total of 17% of the final grade.

Material to study for a miniquiz is very well defined: a miniquiz will cover only the material in problems from the previous two weeks. Miniquiz questions are often simply some parts of these online, class, and pset problems. Students can prepare for a miniquiz simply by reviewing the posted problem solutions for the previous two weeks.

Miniquiz dates are:

1. Feb. 16
2. Mar. 2
3. Mar. 16
4. Apr. 6
5. Apr. 20
6. May 4

Final

There will be a standard 3 hour final exam on **TBA**. This exam is worth 30% of the final course grade.

Grades

The lowest miniquiz score and problem set score, and the lowest two team problem-solving scores will not count in grade calculation. This effectively gives everyone 1 miniquiz, 1 problem set, and 2 team problem-solving sessions they can miss without excuse or penalty.

Grades for the course will be based on the following weighting:

Problem Sets:	25%
Final:	30%
Class participation	20%

Miniquizzes: 17%
Weekly Reading Comments: 3%
Online Tutor Problems: 5%

Note that missed credit (up to a cap of 50%) on problem sets spills over as increased weight of the final and selected quizzes as explained in the [Problem Sets](#) section above.

Email Forum

Email to

[6042-forum\(at\)csail.mit.edu](mailto:6042-forum(at)csail.mit.edu)

will broadcast to all students and staff.

The forum is intended for general course-related communication by class members. We encourage students to use it to arrange study sessions, discuss homework, and send comments to the entire class. The staff also emails announcements and corrections to this list.

General information about the mailing list, including subscribe/unsubscribe instructions, is at:

<http://lists.csail.mit.edu/mailman/listinfo/6042-forum>

Questions, Suggestions, and Complaints

In addition to the forum, email can be sent to the staff or to individual staff members using the addresses on the [staff contact page](#).

Latex macros

Course handouts are formatted using LaTeX, which is the preferred formatting system among Mathematics professionals. Note that we do not think it's worthwhile for students to use it for their class submissions.

For website issues, contact the [6042-webmaster\(at\)csail.mit.edu](mailto:6042-webmaster(at)csail.mit.edu)



6.042 lectures & problems by Prof. Albert R Meyer is licensed under a [Creative Commons Attribution-NonCommercial-Share Alike 3.0 United States License](#).

This document last modified Wednesday, 02-Feb-2011 22:19:11 EST

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Mathematics for Computer Science
6.042J/18.062J

<http://courses.csail.mit.edu/6.042>

WELCOME!
Prof. Albert R Meyer

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Quick Summary

1. Fundamental Concepts of Discrete Mathematics (*sets, relations, proof methods,...*)
2. Discrete Mathematical Structures (*graphs, trees, counting...*)
3. Discrete Probability Theory

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Vocabulary

Quickie:
What does "discrete" mean?
(\neq "discreet")

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Online Tutor Registration

- TP.1: Registration asap
- not later than
Saturday, 9AM
for table assignment

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Reading Assignment

- Courseinfo on web page asap
- Notes Chapters 1 & 2 asap
- Ch. 3, 4.1–4.7 next week
- Email Reading Comments
--due dates in tutor TP.2

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Course Web site

<http://courses.csail.mit.edu/6.042>

- announcements
- class schedule
- notes, slides,...
- course organization
- grading info

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Lecture & Team Problems

Three 1.5 hour class sessions:
 • 1/2 hour overview lecture,
 • then team problem-solving.

Team participation counts
 20% of final grade
 Teams assigned by Monday

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Active Lectures

Say "hello" to your
 neighbors —you'll be
 working with them

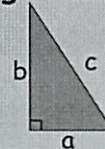
6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Active Lectures

Quickie question:
 Where was your
 neighbor born?

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Getting started: Pythagorean theorem



$$a^2 + b^2 = c^2$$

Familiar? Yes!
 Obvious? No!

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

A Cool Proof

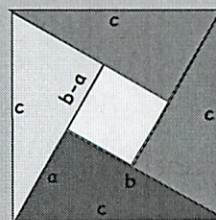


Rearrange into:

- (i) a $c \times c$ square, and then
- (ii) an $a \times a$ & a $b \times b$ square

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

A Cool Proof



6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

A Cool Proof

Albert R. Meyer, 2011 February 2, 2011 lec 1W.15

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

A False Proof: Getting Rich By Diagram

Albert R. Meyer, 2011 February 2, 2011 lec 1W.16

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

A False Proof: Getting Rich By Diagram

Albert R. Meyer, 2011 February 2, 2011 lec 1W.17

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Getting Rich

The bug:

 are not right triangles!
 So the top and bottom line of the "rectangle" is not straight!

Albert R. Meyer, 2011 February 2, 2011 lec 1W.18

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

1 = -1 ?

pictures are not the only source of false proofs

$$1 = \sqrt{1} = \sqrt{(-1)(-1)} = \sqrt{-1}\sqrt{-1} = (\sqrt{-1})^2 = -1$$

Moral:

1. Calculation is a risky substitute for understanding.
2. Be sure you know the rules.

Albert R. Meyer, 2011 February 2, 2011 lec 1W.23

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Consequences of 1 = -1

$$\frac{1}{2} = -\frac{1}{2} \quad (\text{multiply by } \frac{1}{2})$$

$$2 = 1 \quad (\text{add } \frac{3}{2})$$

"Since I and the Pope are clearly 2, we conclude that I and the Pope are 1. That is, I am the Pope."
 -- Bertrand Russell

Albert R. Meyer, 2011 February 2, 2011 lec 1W.25

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Consequences of $1 = -1$



Bertrand Russell (1872 - 1970)

[Picture source: <https://www.gettyimages.com/detail/photo/bertrand-russell-royal-academy-science-artwork-image118812>]



Albert R. Meyer, 2011

February 2, 2011

lec 1W.2.6

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Team Problems

Problems

1-3



Albert R. Meyer, 2011

February 2, 2011

lec 1W.2.7

Albert Meyer

Creative Commons sticker on slides!

(Finally a "real" class)

1. Fundamental concepts discrete math

- set relations

- proof methods

(awesome!)

- explain things in a convincing way

- like a spec for a program

2. Discrete Mathematical Structures

- graphs

- trees counting

3. Discrete Probability

(did already)

In Teal room

- start engaging w/ material

- only talks half an hr

Discrete

2

Organized around class website

Also an online tutor

Problem # 1 is a baseline assessment
due Sat 9AM

Read Chap 1 + 2 asap
+ Course info
(Chap 1 by Fri)

Grade team projects on participation

- Online on OCLW - 20% of grade

Send ~~write~~ comment on readings

Do reading before class

Tutor can resubmit as often as you want

3 x 1.5 hr sessions/week

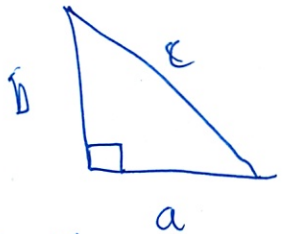
- half hr lecture

- 1 hr solving

Chem

③ What is math?

Pythagorean Theorem



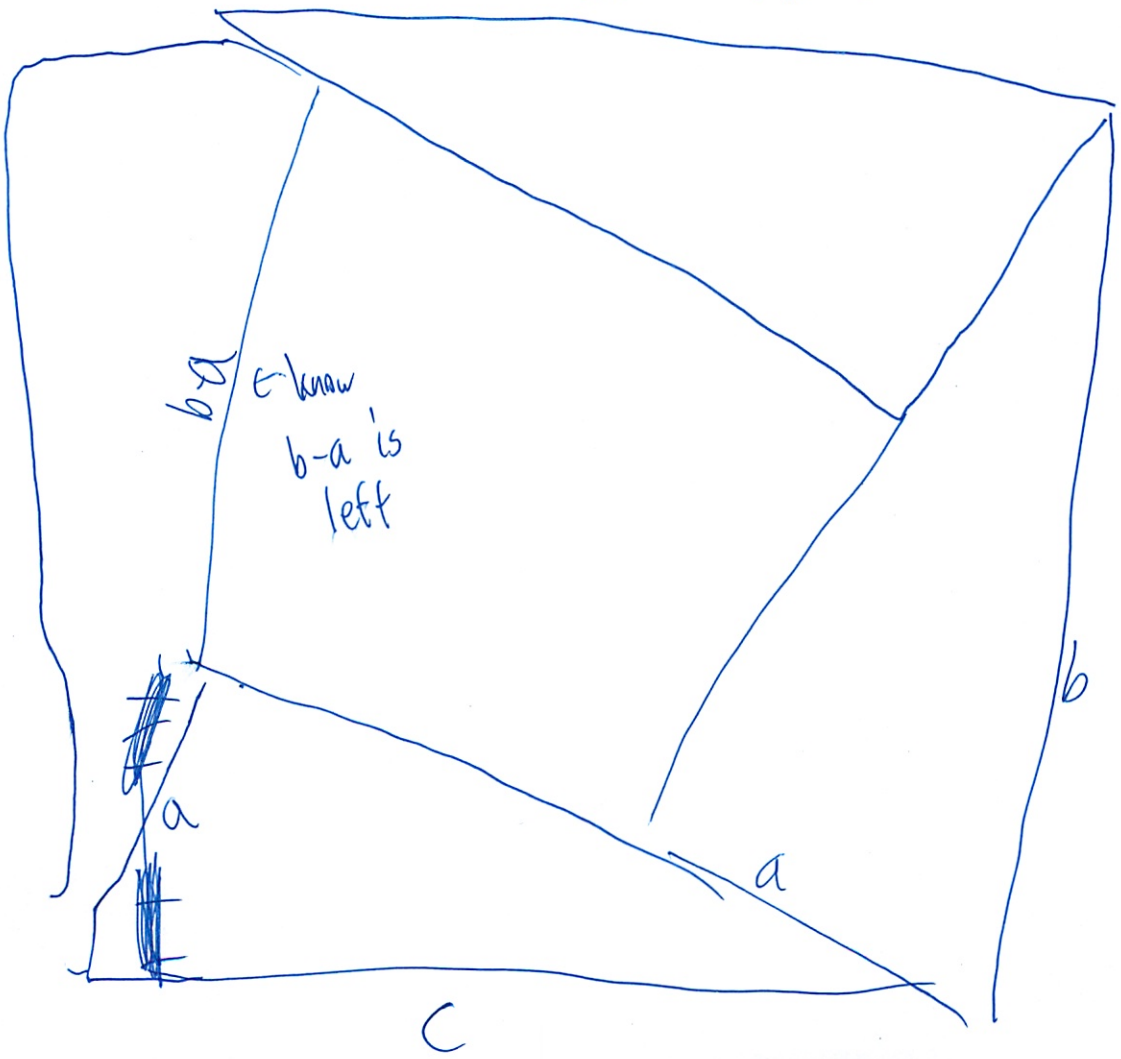
$$a^2 + b^2 = c^2$$

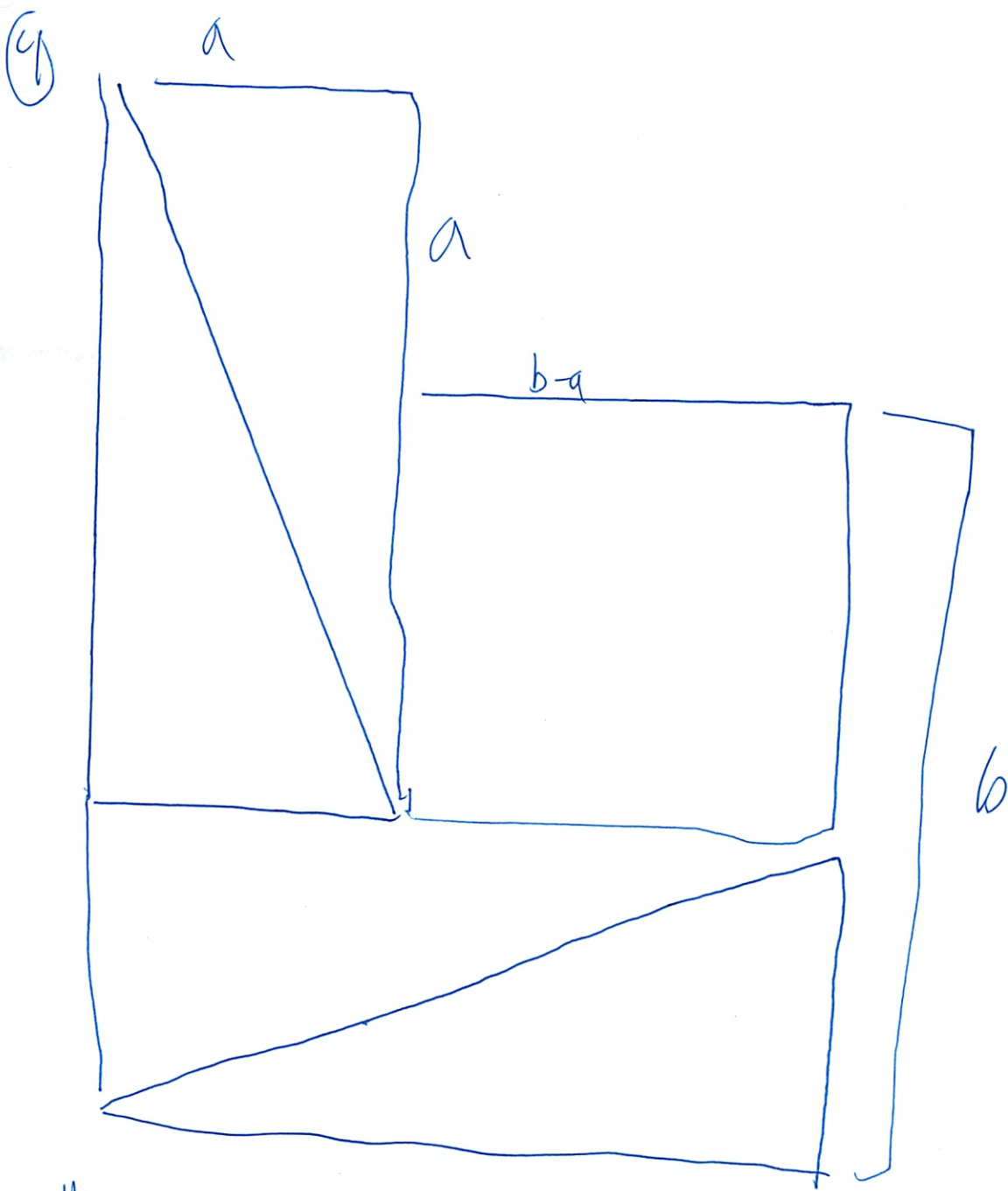
Familiar: Yes

Obvious: No

↳ 200 proofs

C x C square





Mathematicians don't like ~~graphical~~ graphical proofs

- dangerous

- all types of implicit bugs

Showered another proof

- what is the bug?

- won't be a right angle - the little triangles

5) So the lines are not really straight

Pictures are not only false proof

$$1 = \sqrt{1} = \sqrt{(-1)(-1)} = \sqrt{-1}\sqrt{-1} = (-\sqrt{1})^2 = -1$$

↑
is this i or $-i$?

Now team problems

1. $1/8 > 1/4$

$3 > 2$

$3 \log_{10}(1/2) > 2 \log_{10}(1/2)$

Find flaws in proofs

You think you know it
- but less intuitive than it seems
Tricky,

Need to stare + really know math

Write as much as you can, be clear

(Is very tricky!)

(Really need to know math rules)

In-Class Problems Week 1, Wed.

Problem 1.

Identify exactly where the bugs are in each of the following bogus proofs.¹

(a) **Bogus Claim:** $1/8 > 1/4$.

Bogus proof.

$$\begin{aligned}
 3 &> 2 \\
 3 \log_{10}(1/2) &> 2 \log_{10}(1/2) \\
 \log_{10}(1/2)^3 &> \log_{10}(1/2)^2 \\
 (1/2)^3 &> (1/2)^2,
 \end{aligned}$$

is actually other way
log is negative

and the claim now follows by the rules for multiplying fractions.

(b) *Bogus proof:* $1\text{¢} = \$0.01 = (\$0.1)^2 = (10\text{¢})^2 = 100\text{¢} = \1 .

(c) **Bogus Claim:** If a and b are two equal real numbers, then $a = 0$.


Bogus proof.

$$\begin{aligned}
 a &= b \\
 a^2 &= ab \\
 a^2 - b^2 &= ab - b^2 \\
 (a-b)(a+b) &= (a-b)b \\
 a+b &= b \\
 a &= 0.
 \end{aligned}$$

(a-b) divide by 0
here too!
units need to square units as well
a = 5 = b

Multiply by both sides still write

$$\begin{aligned}
 a &= a \\
 a^2 &= a^2 \\
 a^2 - a^2 &= a^2 - a^2 \\
 (a-a)(a+a) &= (a-a)a \\
 a+a &= a \\
 a &= 0 \\
 5 &= 5 \\
 25 &= 25 \\
 25 - 25 &= 25 - 25 \\
 (5-5)(5+5) &= (5-5)5
 \end{aligned}$$

Creative Commons  2011, Eric Lehman, F Tom Leighton, Albert R Meyer.
¹From Stueben, Michael and Diane Sandford. *Twenty Years Before the Blackboard*, Mathematical Association of America, ©1998.

Problem 2.

It's a fact that the Arithmetic Mean is at least as large as the Geometric Mean, namely,

$$\frac{a+b}{2} \geq \sqrt{ab} \quad \text{known}$$

for all nonnegative real numbers a and b . But there's something objectionable about the following proof of this fact. What's the objection, and how would you fix it?

Bogus proof.

Start w/ true statement

$$\frac{a+b}{2} \geq \sqrt{ab}, \quad \text{known by def} \quad \text{so}$$

$$a+b \geq 2\sqrt{ab}, \quad \text{so}$$

$$(a+b)^2 = a^2 + 2ab + b^2 \geq 4ab, \quad \text{so}$$

$$a^2 + 2ab + b^2 \geq 4ab, \quad \text{so}$$

$$a^2 - 2ab + b^2 \geq 0, \quad \text{so}$$

$$(a-b)^2 \geq 0 \quad \text{which we know is true.}$$

The last statement is true because $a-b$ is a real number, and the square of a real number is never negative. This proves the claim. ■

Haven't any question at all - work your way up - backwards, direction is wrong

Problem 3.

Albert announces to his class that he plans to surprise them with a quiz sometime next week.

His students first wonder if the quiz could be on Friday of next next. They reason that it can't: if Albert didn't give the quiz before Friday, then by midnight Thursday, they would know the quiz had to be on Friday, and so the quiz wouldn't be a surprise any more.

not midnight Thu yet when they decide this

Next the students wonder whether Albert could give the surprise quiz Thursday. They observe that if the quiz wasn't given before Thursday, it would have to be given on the Thursday, since they already know it can't be given on Friday. But having figured that out, it wouldn't be a surprise if the quiz was on Thursday either. Similarly, the students reason that the quiz can't be on Wednesday, Tuesday, or Monday. Namely, it's impossible for Albert to give a surprise quiz next week. All the students now relax, having concluded that Albert must have been bluffing.

And since no one expects the quiz, that's why, when Albert gives it on Tuesday next week, it really is a surprise!

What do you think is wrong with the students' reasoning?

no step is wrong but presumes what knowing is lots of worry about that you don't know what you are talking about from a math point of view don't know what surprise means

or if p then q does not imply q then p which is what we are trying to prove

when multiply by neg # sign flips

if would have been in other order it would have been correct

Solutions to In-Class Problems Week 1, Wed.

Problem 1.

Identify exactly where the bugs are in each of the following bogus proofs.¹

(a) **Bogus Claim:** $1/8 > 1/4$.

Bogus proof.

$$\begin{aligned}3 &> 2 \\3 \log_{10}(1/2) &> 2 \log_{10}(1/2) \\ \log_{10}(1/2)^3 &> \log_{10}(1/2)^2 \\ (1/2)^3 &> (1/2)^2,\end{aligned}$$

and the claim now follows by the rules for multiplying fractions. ■

Solution. $\log x < 0$, for $0 < x < 1$, so since both sides of the inequality “ $3 > 2$ ” are being multiplied by the negative quantity $\log_{10}(1/2)$, the “ $>$ ” in the second line should have been “ $<$.” ■

(b) *Bogus proof:* $1\phi = \$0.01 = (\$0.1)^2 = (10\phi)^2 = 100\phi = \1 . ■

Solution. $\$0.01 = \$(0.1)^2 \neq (\$0.1)^2$ because the units $\2 and $\$$ don't match (just as in physics the difference between sec^2 and sec indicates the difference between acceleration and velocity). Similarly, $(10\phi)^2 \neq 100\phi$. ■

(c) **Bogus Claim:** If a and b are two equal real numbers, then $a = 0$.

Bogus proof.

$$\begin{aligned}a &= b \\ a^2 &= ab \\ a^2 - b^2 &= ab - b^2 \\ (a - b)(a + b) &= (a - b)b \\ a + b &= b \\ a &= 0.\end{aligned}$$

Solution. The bug is at the fifth line: one cannot cancel $(a - b)$ from both sides of the equation on the fourth line because $a - b = 0$. ■

Creative Commons  2011, Eric Lehman, F Tom Leighton, Albert R Meyer .

¹From Stueben, Michael and Diane Sandford. *Twenty Years Before the Blackboard*, Mathematical Association of America, ©1998.

Problem 2.

It's a fact that the Arithmetic Mean is at least as large the Geometric Mean, namely,

$$\frac{a+b}{2} \geq \sqrt{ab}$$

for all nonnegative real numbers a and b . But there's something objectionable about the following proof of this fact. What's the objection, and how would you fix it?

Bogus proof.

$$\begin{aligned} \frac{a+b}{2} &\stackrel{?}{\geq} \sqrt{ab}, && \text{so} \\ a+b &\stackrel{?}{\geq} 2\sqrt{ab}, && \text{so} \\ a^2 + 2ab + b^2 &\stackrel{?}{\geq} 4ab, && \text{so} \\ a^2 - 2ab + b^2 &\stackrel{?}{\geq} 0, && \text{so} \\ (a-b)^2 &\geq 0 && \text{which we know is true.} \end{aligned}$$

The last statement is true because $a-b$ is a real number, and the square of a real number is never negative. This proves the claim. ■

Solution. In this argument, we started with what we wanted to prove and then reasoned until we reached a statement that is surely true. The little question marks presumably are supposed to indicate that we're not quite certain that the inequalities are valid until we get down to the last step. At that step, the inequality checks out, *but that doesn't prove the claim*. All we have proved is that **if** $(a+b)/2 \geq \sqrt{ab}$, **then** $(a-b)^2 \geq 0$, which is not very interesting, since we already knew that the square of any nonnegative number is nonnegative.

To be fair, this bogus proof is pretty good: if it was written in reverse order—or if “so” was simply replaced by “is implied by” after each line—it would actually prove the Arithmetic-Geometric Mean Inequality:

Proof.

$$\begin{aligned} \frac{a+b}{2} &\geq \sqrt{ab} && \text{is implied by} \\ a+b &\geq 2\sqrt{ab}, && \text{which is implied by} \\ a^2 + 2ab + b^2 &\geq 4ab, && \text{which is implied by} \\ a^2 - 2ab + b^2 &\geq 0, && \text{which is implied by} \\ (a-b)^2 &\geq 0. \end{aligned}$$

The last statement is true because $a-b$ is a real number, and the square of a real number is never negative. This proves the claim. ■

But the problem with the bogus proof as written is that it reasons backward, beginning with the proposition in question and reasoning to a true conclusion. This kind of backward reasoning can easily “prove” false statements. Here's an example:

Bogus Claim: $0 = 1$.

Bogus proof.

$$\begin{array}{ll} 0 \stackrel{?}{=} 1, & \text{so} \\ 1 \stackrel{?}{=} 0, & \text{so} \\ 0 + 1 \stackrel{?}{=} 1 + 0, & \text{so} \\ 1 = 1 & \text{which is trivially true,} \end{array}$$

which proves $0 = 1$. ■

We can also come up with very easy “proofs” of true theorems, for example, here’s an easy “proof” of the Arithmetic-Geometric Mean Inequality:

Bogus proof.

$$\begin{array}{ll} \frac{a+b}{2} \stackrel{?}{\geq} \sqrt{ab}, & \text{so} \\ 0 \cdot \frac{a+b}{2} \stackrel{?}{\geq} 0 \cdot \sqrt{ab}, & \text{so} \\ 0 \geq 0 & \text{which is trivially true.} \blacksquare \end{array}$$

So watch out for backward proofs! ■

Problem 3.

Albert announces to his class that he plans to surprise them with a quiz sometime next week.

His students first wonder if the quiz could be on Friday of next next. They reason that it can’t: if Albert didn’t give the quiz *before* Friday, then by midnight Thursday, they would know the quiz had to be on Friday, and so the quiz wouldn’t be a surprise any more.

Next the students wonder whether Albert could give the surprise quiz Thursday. They observe that if the quiz wasn’t given *before* Thursday, it would have to be given *on* the Thursday, since they already know it can’t be given on Friday. But having figured that out, it wouldn’t be a surprise if the quiz was on Thursday either. Similarly, the students reason that the quiz can’t be on Wednesday, Tuesday, or Monday. Namely, it’s impossible for Albert to give a surprise quiz next week. All the students now relax, having concluded that Albert must have been bluffing.

And since no one expects the quiz, that’s why, when Albert gives it on Tuesday next week, it really is a surprise!

What do you think is wrong with the students’ reasoning?

Solution. The basic problem is that “surprise” is not a mathematical concept, nor is there any generally accepted way to give it a mathematical definition. The “proof” above assumes some plausible axioms about surprise, without defining it. The paradox is that these axioms are inconsistent. But that’s no surprise :–) since, mathematically speaking, we don’t know what we’re talking about.

Mathematicians and philosophers have had a lot more to say about what might be wrong with the students’ reasoning,—see Chow, Timothy Y. *The surprise examination or unexpected hanging paradox*, *American Mathematical Monthly* (January 1998), pp. 41–51. ■

- Simply by hand, no PCs, etc

1. Derivative

$$\frac{d}{dx} x \ln \frac{x}{e} \text{ at } \sqrt{e}$$

idk all the rules

2. Integrate

$$\int_{e^2}^{e^3} \ln x \, dx$$

3. $\overline{5) 4199001.3777778}$

I suppose we can use a calc

$$3172578719955 \left(\frac{3}{5} \right)$$

4. Set theory

- power set:

Weird notation never say

Oh 2^8 elements in the set

I see now

②

3. Union of $A \cup B$ must be = to sum of sizes

- guess yes since size grows exponentially

- Oh have some questions about when

What is intersect symbol? \cap

I should know this from 6.041??

$A \cap B$ is empty - no overlap
and

← answer

Or we are not doing exponential

if $A \in B$ will then just B not true

$A \cap B \neq$ empty some overlap

⊙

5. Math terms

greatest common denominator

- sounds familiar

+ what is it

- make fractions =

prime #

proof by contradiction

- show where false

injective functions

- never lead

③

least upper bound (lub)

- not heard

equivalence relation

- not heard

DeMorgan's law

- not heard

6. Predicate Logic

- which are logic

$$\text{Not } (P \text{ or } Q) = (\text{Not } P) \text{ and } (\text{Not } Q)$$

work it through

$$\text{if } P, Q, P \wedge Q = \text{True} \rightarrow \text{False}$$

$$P \wedge Q = \text{False} \rightarrow \text{True}$$

$$\text{Not } P = \text{False} \rightarrow \text{True}$$

$$Q = \text{False} \rightarrow \text{True}$$

bad notation

(True)

b. P implies Q or Q implies P

False as in class?

But Plus what is or in middle??

4

c) For all x there exists

$$y [P(x) \text{ or } \text{Not } P(y)]$$

What is P?

would say false

d) same for d

x) All always true

7. Summation

$$2 + 4 + 6 + 8 + \dots + 2-2001 + 2-2002$$

what is pattern here?

Oh multiplication signs?

$$\sum_{x=1}^{2002} 2x$$

Wolfram

401000



b)

$$\sum_{n=0}^{19} 2^n$$

Wolfram

1048575



5

8. Combinatorics - what in all world is that?

Which correctly describe the ~~size~~ # of size 3
Subsets of set $\{1, 2, \dots, 6\}$

WP: Countable structure
kind and size

No clue whatsoever

9. Probability

- I ₃ should get this
fair coin

$$P(\text{all 3 heads}) = \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{8}$$

$$b) P(\text{at least 2}) = P(3) + P(2 \text{ heads})$$

$$\frac{1}{8} + \binom{2}{3} \frac{1}{2} \cdot \frac{1}{2}$$

WA=0
↑ wolfram alpha
? that included?

$$\sigma \text{ PPS } \binom{3}{2} = 3$$

$$\frac{1}{2} + 3 \cdot \frac{1}{8} = \frac{1}{2}$$

c) Avg # heads 1.5

done

- I knew some things but not others
- need to remember deriv/int/log rules

Solutions to In-Class Problems Week 1, Wed.

Problem 1.

Identify exactly where the bugs are in each of the following bogus proofs.¹

(a) **Bogus Claim:** $1/8 > 1/4$.

Bogus proof.

$$\begin{aligned}3 &> 2 \\3 \log_{10}(1/2) &> 2 \log_{10}(1/2) \\ \log_{10}(1/2)^3 &> \log_{10}(1/2)^2 \\ (1/2)^3 &> (1/2)^2,\end{aligned}$$

and the claim now follows by the rules for multiplying fractions. ■

Solution. $\log x < 0$, for $0 < x < 1$, so since both sides of the inequality “ $3 > 2$ ” are being multiplied by the negative quantity $\log_{10}(1/2)$, the “ $>$ ” in the second line should have been “ $<$.” ■

(b) *Bogus proof:* $1\text{¢} = \$0.01 = (\$0.1)^2 = (10\text{¢})^2 = 100\text{¢} = \1 . ■

Solution. $\$0.01 = \$(0.1)^2 \neq (\$0.1)^2$ because the units $\2 and $\$$ don't match (just as in physics the difference between sec^2 and sec indicates the difference between acceleration and velocity). Similarly, $(10\text{¢})^2 \neq 100\text{¢}$. ■

*makes sense
now or 2/7*

(c) **Bogus Claim:** If a and b are two equal real numbers, then $a = 0$.

Bogus proof.

$$\begin{aligned}a &= b \\ a^2 &= ab \\ a^2 - b^2 &= ab - b^2 \\ (a - b)(a + b) &= (a - b)b \\ a + b &= b \\ a &= 0.\end{aligned}$$

Solution. The bug is at the fifth line: one cannot cancel $(a - b)$ from both sides of the equation on the fourth line because $a - b = 0$. ■

Nice

Problem 2.

It's a fact that the Arithmetic Mean is at least as large the Geometric Mean, namely,

$$\frac{a+b}{2} \geq \sqrt{ab}$$

for all nonnegative real numbers a and b . But there's something objectionable about the following proof of this fact. What's the objection, and how would you fix it?

Bogus proof.

$$\begin{aligned} \frac{a+b}{2} &\stackrel{?}{\geq} \sqrt{ab}, && \text{so} \\ a+b &\stackrel{?}{\geq} 2\sqrt{ab}, && \text{so} \\ a^2 + 2ab + b^2 &\stackrel{?}{\geq} 4ab, && \text{so} \\ a^2 - 2ab + b^2 &\stackrel{?}{\geq} 0, && \text{so} \\ (a-b)^2 &\geq 0 && \text{which we know is true.} \end{aligned}$$

The last statement is true because $a-b$ is a real number, and the square of a real number is never negative. This proves the claim. ■

Solution. In this argument, we started with what we wanted to prove and then reasoned until we reached a statement that is surely true. The little question marks presumably are supposed to indicate that we're not quite certain that the inequalities are valid until we get down to the last step. At that step, the inequality checks out, *but that doesn't prove the claim*. All we have proved is that **if** $(a+b)/2 \geq \sqrt{ab}$, **then** $(a-b)^2 \geq 0$, which is not very interesting, since we already knew that the square of any nonnegative number is nonnegative.

To be fair, this bogus proof is pretty good: if it was written in reverse order—or if “so” was simply replaced by “is implied by” after each line—it would actually prove the Arithmetic-Geometric Mean Inequality:

Proof.

how am I suppose to see that?

$$\begin{aligned} \frac{a+b}{2} &\geq \sqrt{ab} && \text{is implied by} \\ a+b &\geq 2\sqrt{ab}, && \text{which is implied by} \\ a^2 + 2ab + b^2 &\geq 4ab, && \text{which is implied by} \\ a^2 - 2ab + b^2 &\geq 0, && \text{which is implied by} \\ (a-b)^2 &\geq 0. \end{aligned}$$

The last statement is true because $a-b$ is a real number, and the square of a real number is never negative. This proves the claim. ■

But the problem with the bogus proof as written is that it reasons backward, beginning with the proposition in question and reasoning to a true conclusion. This kind of backward reasoning can easily “prove” false statements. Here's an example:

Bogus Claim: $0 = 1$.

** Start w/ true*

Bogus proof.

$$\begin{array}{ll} 0 \stackrel{?}{=} 1, & \text{so} \\ 1 \stackrel{?}{=} 0, & \text{so} \\ 0 + 1 \stackrel{?}{=} 1 + 0, & \text{so} \\ 1 = 1 & \text{which is trivially true,} \end{array}$$

which proves $0 = 1$. ■

We can also come up with very easy “proofs” of true theorems, for example, here’s an easy “proof” of the Arithmetic-Geometric Mean Inequality:

Bogus proof.

$$\begin{array}{ll} \frac{a+b}{2} \stackrel{?}{\geq} \sqrt{ab}, & \text{so} \\ 0 \cdot \frac{a+b}{2} \stackrel{?}{\geq} 0 \cdot \sqrt{ab}, & \text{so} \\ 0 \geq 0 & \text{which is trivially true.} \blacksquare \end{array}$$

So watch out for backward proofs! ■

Problem 3.

Albert announces to his class that he plans to surprise them with a quiz sometime next week.

His students first wonder if the quiz could be on Friday of next next. They reason that it can’t: if Albert didn’t give the quiz *before* Friday, then by midnight Thursday, they would know the quiz had to be on Friday, and so the quiz wouldn’t be a surprise any more.

Next the students wonder whether Albert could give the surprise quiz Thursday. They observe that if the quiz wasn’t given *before* Thursday, it would have to be given *on* the Thursday, since they already know it can’t be given on Friday. But having figured that out, it wouldn’t be a surprise if the quiz was on Thursday either. Similarly, the students reason that the quiz can’t be on Wednesday, Tuesday, or Monday. Namely, it’s impossible for Albert to give a surprise quiz next week. All the students now relax, having concluded that Albert must have been bluffing.

And since no one expects the quiz, that’s why, when Albert gives it on Tuesday next week, it really is a surprise!

What do you think is wrong with the students’ reasoning?

Solution. The basic problem is that “surprise” is not a mathematical concept, nor is there any generally accepted way to give it a mathematical definition. The “proof” above assumes some plausible axioms about surprise, without defining it. The paradox is that these axioms are inconsistent. But that’s no surprise :-) since, mathematically speaking, we don’t know what we’re talking about.

Mathematicians and philosophers have had a lot more to say about what might be wrong with the students’ reasoning,—see Chow, Timothy Y. *The surprise examination or unexpected hanging paradox*, American Mathematical Monthly (January 1998), pp. 41–51. ■

I don't like their answer

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Mathematics for Computer Science
MIT 6.042J/18.062J

Proof by Contradiction

Proof by Cases

Albert R Meyer February 4, 2011 lec 1F.1

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Proof by Contradiction

Is $\sqrt[3]{1332} \leq 11$?

If so, $1332 \leq 1331$

That's not true, so

$\sqrt[3]{1332} > 11$

Albert R Meyer February 4, 2011 lec 1F.3

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Proof by Contradiction

If an assertion implies something false, then the assertion itself must be false!

Albert R Meyer February 4, 2011 lec 1F.4

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Proof by Contradiction

Theorem: $\sqrt{2}$ is irrational.

- Suppose $\sqrt{2}$ was rational
- So have n, d integers without common prime factors such that

$$\sqrt{2} = \frac{n}{d}$$
- We will show that n & d are both even. This contradicts no common factor.

Albert R Meyer February 4, 2011 lec 1F.5

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Proof by Contradiction

Theorem: $\sqrt{2}$ is irrational.

so can assume

$\sqrt{2} = \frac{n}{d}$ $\sqrt{2}d = n$ $2d^2 = n^2$ <p>So n is even</p>	$n = 2k$ $n^2 = 4k^2$ $2d^2 = 4k^2$ $d^2 = 2k^2$ <p>So d is even</p>
--	---

Albert R Meyer February 4, 2011 lec 1F.6

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Quickie

Proof assumes that if n^2 is even, then n is even.

Why is this true?

Albert R Meyer February 4, 2011 lec 1F.7

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Mathematics for Computer Science
MIT 6.042J/18.062J

Proof by Cases



Albert R Meyer

February 4, 2011

lec 1F.8

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Java Logical Expression

if ((x>0) || (x <= 0 && y>100))
OR : AND
(more code)

better: if ((x>0) || y>100)
:
(more code)



Albert R Meyer

February 4, 2011

lec 1F.9

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Case 1: $x > 0$

true
if ((x>0) || (x <= 0 && y>100))
OR AND

true
if ((x>0) || y>100)
OR
so both are true



Albert R Meyer

February 4, 2011

lec 1F.10

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Case 2: $x \leq 0$

false
if ((x>0) || (x <= 0 && y>100))
OR AND

false
if ((x>0) || y>100)
OR



Albert R Meyer

February 4, 2011

lec 1F.11

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Case 2: $x \leq 0$

true
if (x <= 0 && y>100)
AND

if (y>100)



Albert R Meyer

February 4, 2011

lec 1F.12

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Case 2: $x \leq 0$

if (y>100)

if (y>100)

so both still the same



Albert R Meyer

February 4, 2011

lec 1F.13

6	9	13	7
12		10	5
3	1	4	14
15	8	11	2

Proof by Cases

Reasoning by cases can break a complicated problem into easier subproblems. Some philosophers* think reasoning this way is worrisome.

*intuitionists



Albert R Meyer

February 4, 2011

lec 1F.25

6	9	13	7
12		10	5
3	1	4	14
15	8	11	2

\$1,000,000 Question

Is $P = NP$?



Albert R Meyer

February 4, 2011

lec 2M.28

6	9	13	7
12		10	5
3	1	4	14
15	8	11	2

\$1,000,000 Question

The answer is on my desk!
(Proof by Cases)



Albert R Meyer

February 4, 2011

lec 1F.30

6	9	13	7
12		10	5
3	1	4	14
15	8	11	2

Team Problems

Problems
1–4



Albert R Meyer

February 4, 2011

lec 1F.31

Proof by Contradiction

- Starting to talk about proof techniques
- Proof by contradiction complicated

~~Proof by force~~

$$\text{is } \sqrt[3]{1332} \leq 11?$$

if no calc

So cube both sides

$$1332 \leq 11^3$$

$$1332 \leq 1331$$

fails - not true!

So it must go the other way so

$$\sqrt[3]{1332} > 11$$

rational = quotient of integers

Thorm: $\sqrt{2}$ is irrational

Suppose $\sqrt{2}$ is rational

Then we have n, d integers w/o common prime factors

Such that $\sqrt{2} = \frac{n}{d}$

②

But we can show n & d are both even

This contradicts that there is no common factor

$$\sqrt{2} = \frac{n}{d}$$

First get rid of fraction

$$\sqrt{2} d = n$$

$$2d^2 = n^2$$

n is even \Rightarrow ? So must be even

So n must be even

So can assume n is twice something (by def)

$$n = 2k$$

Square to match

$$n^2 = 4k^2$$

$$2d^2 = \cancel{4k^2} 4k^2$$

Cancel 2s

$$d^2 = 2k^2$$

So must be \uparrow even \uparrow even

So d is even

3

Proof assumes that if n^2 is even then n is even
Why is this true?

Odd $\stackrel{\text{def}}{\rightarrow} 2d+1$

Square $\rightarrow 4d^2 + 1 \rightarrow$ Still odd

Contradicts ...

Proof by Cases

have some java notation

if $((x > 0) \parallel (x \leq 0 \ \&\& \ y > 100))$

\uparrow
I am bad at ampersands

same as

if $((x > 0) \parallel y > 100)$

Messy to prove so break up into cases
Prove each case

Case 1 $x > 0$

(same as notes)

(prob best not to try + copy -
- follow his logic)

When part of or is false - ignore

4

Must make sure all cases
have

Famous Comp Sci q: Is $P = NP$
↑ polynomial time ↑ nondeterministic polynomial time

Answer is either yes or no

Prob 1

Problems (self + group)

by contradiction

$$a \leq \sqrt{n} \text{ or } b \leq \sqrt{n}$$

both ~~a~~ and $b > \sqrt{n}$

Show that can't be true

$$a \cdot b = n$$

$$a = \frac{n}{b}$$

Since $b > \sqrt{n}$ then

$$\frac{n}{b} < \frac{n}{\sqrt{n}} = \sqrt{n}$$

$$\left\{ \begin{array}{l} \frac{n}{b} < \sqrt{n} \\ a < \sqrt{n} \end{array} \right.$$

Q5

Contradict's $a > \sqrt{n}$

So not true

So thus $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$ is true

#2.

$\frac{1}{4}$

If both even - not in lowest term

If we can divide by 2 then it is not lowest term

another way

Suppose $a, b > \sqrt{n}$

Let $a = (\sqrt{n} + \epsilon_a)$; $b = (\sqrt{n} + \epsilon_b)$ for $\epsilon_a, \epsilon_b > 0$

$$\begin{aligned} a \cdot b &= (\sqrt{n} + \epsilon_a)(\sqrt{n} + \epsilon_b) \\ &= n + \sqrt{n}(\epsilon_a + \epsilon_b) + \epsilon_a \epsilon_b > n \end{aligned}$$

⑥

3. Why does it say $\sqrt{2}^{\sqrt{2}}$ - I thought never rely on \neq

- Case 1 rational
- 2 irrational

#2 else

Suppose $2^{p/q}$ can be written in the form $\frac{n}{d}$
for coprime integers (n, d) and (p, q)

$$\text{Then } 2^{p/q} = \frac{n}{d}$$

$$\text{Implies } d \cdot 2^{p/q} = n$$

(erased)

$$\text{Implies } d^q \cdot 2^p = n^q$$

$$\text{Implies } 2^p \mid n^q$$

So $2 \mid n$ which means $n = 2k$ for $k \in \mathbb{Z}$

$$d^q \cdot 2^p = (2k)^q$$

$$\text{So } d^q \cdot 2^p = 2^q k^q$$

$\rightarrow 2 \mid d$ so d, n are both even

contradicting the coprime assumption

(I totally don't get this)

(Not learning anything - strongly dislike group work)

7

(I learn by going step by step

Very bad to do off students who may not be right)
(got frustrated and snapped at TA!)

Find that
2. Nth root of 2 is not rational

Coprime - n, d , have no factors other than 1
~~the~~ $\frac{n}{d}$ is in lowest form
gcf is 1

Always write what contradiction is

#2 on board instead

For some Ath root of 2, suppose

$\sqrt[A]{2}$ can be written in the form $\frac{n}{d}$, so

$$d^A \sqrt[A]{2} = n$$

$$2 d^A = n^A \rightarrow n^A \text{ is even, } n \text{ can be written}$$

$$2 d^A = 2^A k^A$$

$$n = 2k \\ k \in \mathbb{Z}$$

$$d^A = 2^{A-1} k^A \text{ for some } A \in \mathbb{Z} \geq 1$$

d^A is even
Thus d is even

8

$\therefore n$ and d are both even

Contradiction \square

3 on board $\sqrt{2}$ is irrational

Case 1 $\sqrt{2}^{\sqrt{2}}$ is rational

\rightarrow
we don't
know which
it is
so try both

because $\sqrt{2}$ is irrational, this implies
that an irrational $\#$ to an irrational power
can be rational

Case 2 $\sqrt{2}^{\sqrt{2}}$ is irrational

$$(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\sqrt{2} \cdot \sqrt{2}} = \sqrt{2}^2 = 2$$

because $\sqrt{2}^{\sqrt{2}}$ is assumed to be irrational
and $\sqrt{2}$ is irrational

this implies that an irrational $\#$ to an
irrational power can be rational

(showed a case where it can be true
and true in both cases - so is true)

(I think I am starting to get this - a lot of heuristic

Prof: (make sure can use words) work backwards
worse by than everyone else)

In-Class Problems Week 1, Fri.

Problem 1.

Prove that if $a \cdot b = n$, then a or b must be $\leq \sqrt{n}$, where a, b , and n are nonnegative integers. *Hint:* by contradiction

Problem 2.

Generalize the proof of Theorem 1.8.1 repeated below that $\sqrt{2}$ is irrational. For example, how about $\sqrt[3]{2}$? Remember that an irrational number is a number that cannot be expressed as a ratio of two integers.

Theorem. $\sqrt{2}$ is an irrational number.

Proof. The proof is by contradiction: assume that $\sqrt{2}$ is rational, that is,

$$\sqrt{2} = \frac{n}{d}, \quad (1)$$

where n and d are integers. Now consider the smallest such positive integer denominator, d . We will prove in a moment that the numerator, n , and the denominator, d , are both even. This implies that

$$\frac{n/2}{d/2}$$

is a fraction equal to $\sqrt{2}$ with a smaller positive integer denominator, a contradiction.

Since the assumption that $\sqrt{2}$ is rational leads to this contradiction, the assumption must be false. That is, $\sqrt{2}$ is indeed irrational. This italicized comment on the implication of the contradiction normally goes without saying, but since this is an early example of proof by contradiction, we've said it.

To prove that n and d have 2 as a common factor, we start by squaring both sides of (1) and get $2 = n^2/d^2$, so

$$2d^2 = n^2. \quad (2)$$

So 2 is a factor of n^2 , which is only possible if 2 is in fact a factor of n .

This means that $n = 2k$ for some integer, k , so

$$n^2 = (2k)^2 = 4k^2. \quad (3)$$

Combining (2) and (3) gives $2d^2 = 4k^2$, so

$$d^2 = 2k^2. \quad (4)$$

So 2 is a factor of d^2 , which again is only possible if 2 is in fact also a factor of d , as claimed. ■

Problem 3.

If we raise an irrational number to an irrational power, can the result be rational? Show that it can by considering $\sqrt{2}^{\sqrt{2}}$ and arguing by cases.

Problem 4.

Here is a different proof that $\sqrt{2}$ is irrational, taken from the American Mathematical Monthly, v.116, #1, Jan. 2009, p.69:

Proof. Suppose for the sake of contradiction that $\sqrt{2}$ is rational, and choose the least integer, $q > 0$, such that $(\sqrt{2} - 1)q$ is a nonnegative integer. Let $q' ::= (\sqrt{2} - 1)q$. Clearly $0 < q' < q$. But an easy computation shows that $(\sqrt{2} - 1)q'$ is a nonnegative integer, contradicting the minimality of q . ■

(a) This proof was written for an audience of college teachers, and at this point it is a little more concise than desirable. Write out a more complete version which includes an explanation of each step.

(b) Now that you have justified the steps in this proof, do you have a preference for one of these proofs over the other? Why? Discuss these questions with your teammates for a few minutes and summarize your team's answers on your whiteboard.

Solutions to In-Class Problems Week 1, Fri.

Problem 1.

Prove that if $a \cdot b = n$, then a or b must be $\leq \sqrt{n}$, where a, b , and n are nonnegative integers. *Hint:* by contradiction

Solution. *Proof.* Suppose to the contrary that $a > \sqrt{n}$ and $b > \sqrt{n}$. Then

$$a \cdot b > \sqrt{n} \cdot \sqrt{n} = n,$$

contradicting the fact that $a \cdot b = n$. ■

Problem 2.

Generalize the proof of Theorem 1.8.1 repeated below that $\sqrt{2}$ is irrational. For example, how about $\sqrt[3]{2}$? Remember that an irrational number is a number that cannot be expressed as a ratio of two integers.

Theorem. $\sqrt{2}$ is an irrational number.

Proof. The proof is by contradiction: assume that $\sqrt{2}$ is rational, that is,

$$\sqrt{2} = \frac{n}{d}, \tag{1}$$

where n and d are integers. Now consider the smallest such positive integer denominator, d . We will prove in a moment that the numerator, n , and the denominator, d , are both even. This implies that

$$\frac{n/2}{d/2}$$

is a fraction equal to $\sqrt{2}$ with a smaller positive integer denominator, a contradiction.

Since the assumption that $\sqrt{2}$ is rational leads to this contradiction, the assumption must be false. That is, $\sqrt{2}$ is indeed irrational. This italicized comment on the implication of the contradiction normally goes without saying, but since this is an early example of proof by contradiction, we've said it.

To prove that n and d have 2 as a common factor, we start by squaring both sides of (1) and get $2 = n^2/d^2$, so

$$2d^2 = n^2. \tag{2}$$

So 2 is a factor of n^2 , which is only possible if 2 is in fact a factor of n .

This means that $n = 2k$ for some integer, k , so

$$n^2 = (2k)^2 = 4k^2. \tag{3}$$

Combining (2) and (3) gives $2d^2 = 4k^2$, so

$$d^2 = 2k^2. \quad (4)$$

So 2 is a factor of d^2 , which again is only possible if 2 is in fact also a factor of d , as claimed. ■

Solution. *Proof.* We prove that for any $n > 1$, $\sqrt[n]{2}$ is irrational by contradiction.

Assume that $\sqrt[n]{2}$ is rational. Under this assumption, there exist integers a and b with $\sqrt[n]{2} = a/b$, where b is the smallest such positive integer denominator. Now we prove that a and b are both even, so that

$$\frac{a/2}{b/2}$$

is a fraction equal to $\sqrt[n]{2}$ with a smaller positive integer denominator, a contradiction.

$$\begin{aligned} \sqrt[n]{2} &= \frac{a}{b} \\ 2 &= \frac{a^n}{b^n} \\ 2b^n &= a^n. \end{aligned}$$

The lefthand side of the last equation is even, so a^n is even. This implies that a is even as well (see below for justification).

In particular, $a = 2c$ for some integer c . Thus,

$$\begin{aligned} 2b^n &= (2c)^n = 2^n c^n, \\ b^n &= 2^{n-1} c^n. \end{aligned}$$

Since $n - 1 > 0$, the righthand side of the last equation is an even number, so b^n is even. But this implies that b must be even as well, contradicting the fact that a/b is in lowest terms. ■

Now we justify the claim that if a^n is even, so is a .

There is a simple proof by contradiction: suppose to the contrary that a is odd. It's a familiar (and easily verified¹) fact that the product of two odd numbers is odd, from which it follows that the product of *any* finite number of odd numbers is odd, so a^n would also be odd, contradicting the fact that a^n is even.

More generally for *any* integers $m, k > 0$, if m^k is divisible by a prime number, p , then m must be divisible by p . This follows from the factorization of an integer into primes (which we'll discuss further in a coming lecture): the primes in the factorization of m^k are precisely the primes in the factorization of m repeated k times, so if there is a p in the factorization of m^k it must be one of k copies of a p in the factorization of m . ■

Problem 3.

If we raise an irrational number to an irrational power, can the result be rational? Show that it can by considering $\sqrt{2}^{\sqrt{2}}$ and arguing by cases.

Solution. We want to find irrational numbers a, b such that a^b is rational. We argue by cases.

Case 1: [$\sqrt{2}^{\sqrt{2}}$ is rational]. Let $a = b = \sqrt{2}$. a and b are irrational since $\sqrt{2}$ is irrational as we know. Also, a^b is rational by case hypothesis. So we have found the required a and b in this case.

¹Two odd integers can be written as $2x + 1$ and $2y + 1$ for some integers x and y . Then their product is also odd because it equals $2z + 1$ where $z = 2(2xy + x + y) + 1$.

Case 2: [$\sqrt{2}\sqrt{2}$ is irrational]. Let $a = \sqrt{2}\sqrt{2}$ and $b = \sqrt{2}$. Then a is irrational by case hypothesis, we know b is irrational, and

$$a^b = \left(\sqrt{2}\sqrt{2}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^2 = 2,$$

which is rational. So we have found the required a and b in this case also.

So in any case, there will be irrational a, b such that a^b is rational. Note that we have no clue about which case is true, but that didn't matter. ■

Problem 4.

Here is a different proof that $\sqrt{2}$ is irrational, taken from the American Mathematical Monthly, v.116, #1, Jan. 2009, p.69:

Proof. Suppose for the sake of contradiction that $\sqrt{2}$ is rational, and choose the least integer, $q > 0$, such that $(\sqrt{2} - 1)q$ is a nonnegative integer. Let $q' ::= (\sqrt{2} - 1)q$. Clearly $0 < q' < q$. But an easy computation shows that $(\sqrt{2} - 1)q'$ is a nonnegative integer, contradicting the minimality of q . ■

(a) This proof was written for an audience of college teachers, and at this point it is a little more concise than desirable. Write out a more complete version which includes an explanation of each step.

Solution. The points that need justification are:

1. Why is there a positive integer, q , such that $(\sqrt{2} - 1)q$ is a nonnegative integer? *Answer:* Since $\sqrt{2}$ is rational, so is $\sqrt{2} - 1$. So $\sqrt{2} - 1$ can be expressed as an integer quotient with positive denominator; now just let q be that denominator.
2. Why is there such a *least* positive integer, q ? *Answer:* As long as there is one such positive integer, there has to be a least one. This obvious fact is known as the *Well Ordering Principle*.
3. Why is $0 < q' < q$? *Answer:* We know that $1 < \sqrt{2} < 2$, so $0 < \sqrt{2} - 1 < 1$. Therefore, $0 < (\sqrt{2} - 1)r < r$ for any real number $r > 0$.
4. Why is $(\sqrt{2} - 1)q'$ a nonnegative integer? *Answer:* It's actually positive, because it is a product of positive numbers. It's integer because

$$(\sqrt{2} - 1)q' = (\sqrt{2} - 1)^2 q = 2q - 2q\sqrt{2} + q = q - 2 \cdot [(\sqrt{2} - 1)q]$$

and the last term is of the form (integer $- 2 \cdot$ [integer]). ■

(b) Now that you have justified the steps in this proof, do you have a preference for one of these proofs over the other? Why? Discuss these questions with your teammates for a few minutes and summarize your team's answers on your whiteboard.

Solution. Both proofs seem about equally easy to understand. The previous problems shows that the first proof generalizes pretty directly from square roots to k th roots, which doesn't seem as clear for the this second proof. On the other hand, the first proof requires appeal to Unique Prime Factorization, while the second just uses simple algebra. ■

TP.2.1

answer as series of integers

$$p(n) = n^2 + n + 41$$

↑function or preposition?

a) What are primes ≤ 41

- just look up online (✓)

b) Factors of $p(41)$

$$41^2 + 41 + 41 = ~~4363~~ 1763$$

↑How get factors

Call in wolfram?

$$41 \times 43$$

↑but how do manually? (✓)

c) To verify $p(39)$ is prime, you can check that not divisible by any prime $\leq n$

What is smallest n this will work?

- well less than half

$$39^2 + 39 + 41 = 1601$$

②

$$\frac{1601}{2} = 800.5$$

800 (X)

Some prime check formula \rightarrow book 2.4
does not really describe a good formula

- skip
- credit only for trying

WP: Primality test

- only need to test up to \sqrt{n} , round down

- so 40 (✓)

Or just check 2!

(6k + 1)

(This algorithm stuff is fun!)

~~try~~
Gets complex \rightarrow skipping

TP 2.2 Bogus well ordering proof

$F(n) = n$ th fib #

$F(n) = F(n-1) + F(n-2)$

Trying to claim each fib # is even

③

Is the sum of 2 even #'s even?

- I think

Something seems wrong - but what?

- using QED?

- Summing 2 odds can give even

Answer

γ and \parallel

- \parallel = final state

Proof only shows min $m \in C$ is not 0

and assumption $m \geq 2$ is contradiction

↳ was thinking that

- Unexamined case $m=1$ and $1 \in C$

- need to handle case $\nexists(1)$

$\uparrow 1$ is a member of C

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Mathematics for Computer Science
MIT 6.042J/18.062J

The Well Ordering Principle

This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License.

Albert R Meyer February 7, 2011 Lec 2M.1

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Well Ordering principle

Every nonempty set of
nonnegative integers
has a
least element.

Familiar? Now you mention it, Yes.
Obvious? Yes.
Trivial? Yes. But watch out:

Albert R Meyer February 7, 2011 Lec 2M.2

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Well Ordering principle

Every nonempty set of
nonnegative rationals
has a
least element.

NO!

Albert R Meyer February 7, 2011 Lec 2M.3

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Well Ordering principle



Every nonempty set of
~~*nonnegative integers*~~
has a
least element.

NO!

Albert R Meyer February 7, 2011 Lec 2M.4

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Well Ordered Postage

available stamps:  



5¢ 3¢

Thm: Get any amount $n \geq 8¢$
Prove by WOP. Suppose not.
Let m be least counterexample.

Albert R Meyer February 7, 2011 Lec 2M.11

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Well Ordered Postage

available stamps:  


5¢ 3¢


So, cannot make $m¢$.
can make any amount $< m$,
and $\underline{\underline{\geq 8}}$


Albert R Meyer February 7, 2011 Lec 2M.12

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Well Ordered Postage

$m > 8$: 

$m > 9$: 

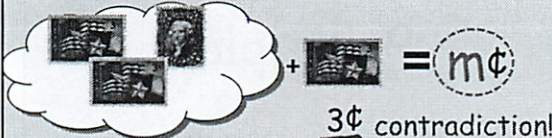
$m > 10$: 

Albert R Meyer February, 7, 2011 Lec 2M.14

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Well Ordered Postage

So $m \geq 11$. Now $m > m-3 \geq 8$
so can get $m-3\text{¢}$. But



$m-3\text{¢} + 3\text{¢} = m\text{¢}$
3¢ contradiction!

Albert R Meyer February, 7, 2011 Lec 2M.15

add back 3 cents

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Geometric sums

$$1 + r + r^2 + r^3 + \dots + r^n = \frac{r^{n+1} - 1}{r - 1}$$

Proof by WOP. Let m be smallest n with \neq . But $=$ for $n = 0$, so $m > 0$, and

$$1 + r + r^2 + r^3 + \dots + r^{m-1} = \frac{r^m - 1}{r - 1}$$

Albert R Meyer February, 7, 2011 Lec 2M.16

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Geometric sums

$$1 + r + r^2 + r^3 + \dots + r^{m-1} = \frac{r^m - 1}{r - 1}$$

add r^m to both sides

$$\text{LHS} = 1 + r + r^2 + r^3 + \dots + r^{m-1} + r^m$$

$$\text{RHS} = \frac{r^m - 1}{r - 1} + \frac{r^{m+1} - r^m}{r - 1} = \frac{r^{m+1} - 1}{r - 1}$$

so $=$ at m , contradicting \neq :
there is no counterexample.

Albert R Meyer February, 7, 2011 Lec 2M.17

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Well Ordering Principle Proofs

To prove $\forall n \in \mathbb{N}. P(n)$ using WOP:

- define set of counterexamples
 $C ::= \{n \in \mathbb{N} \mid \text{NOT } P(n)\}$
- assume C is not empty. By WOP, have minimum element $m \in C$
- Reach a contradiction *somehow* ...
usually by proving $P(m)$ with $c < m$

Albert R Meyer February, 7, 2011 Lec 2M.18

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Team Problems

Problems

1-4

Albert R Meyer February, 7, 2011 Lec 2M.19

In-Class Problems Week 2, Mon.

Problem 1.

The proof below uses the Well Ordering Principle to prove that every amount of postage that can be assembled using only 6 cent and 15 cent stamps, is divisible by 3. Let the notation " $j \mid k$ " indicate that integer j is a divisor of integer k , and let $S(n)$ mean that exactly n cents postage can be assembled using only 6 and 15 cent stamps. Then the proof shows that

$$S(n) \text{ IMPLIES } 3 \mid n, \quad \text{for all nonnegative integers } n. \quad (*)$$

Fill in the missing portions (indicated by "...") of the following proof of (*).

Let C be the set of *counterexamples* to (*), namely¹

$$C ::= \{n \mid \dots\} \quad \downarrow \text{will show false}$$

Assume for the purpose of obtaining a contradiction that C is nonempty. Then by the WOP, there is a smallest number, $m \in C$. This m must be positive because (1) 0 works, not a counterexample

But if $S(m)$ holds and m is positive, then $S(m-6)$ or $S(m-15)$ must hold, because (2) Others must be pos

So suppose $S(m-6)$ holds. Then $3 \mid (m-6)$, because (3)

But if $3 \mid (m-6)$, then obviously $3 \mid m$, contradicting the fact that m is a counterexample.

Next, if $S(m-15)$ holds, we arrive at a contradiction in the same way. Since we get a contradiction in both cases, we conclude that (4)

which proves that (*) holds.

Problem 2.

Use the Well Ordering Principle to prove that

$$\sum_{k=0}^n k^2 = \frac{n(n+1)(2n+1)}{6}. \quad (1)$$

for all nonnegative integers, n .

Problem 3.

Euler's Conjecture in 1769 was that there are no positive integer solutions to the equation

$$a^4 + b^4 + c^4 = d^4.$$

Integer values for a, b, c, d that do satisfy this equation, were first discovered in 1986. So Euler guessed wrong, but it took more two hundred years to prove it.

Now let's consider Lehman's equation, similar to Euler's but with some coefficients:

$$8a^4 + 4b^4 + 2c^4 = d^4 \quad (2)$$

Prove that Lehman's equation (2) really does not have any positive integer solutions.

Hint: Consider the minimum value of a among all possible solutions to (2).

How to prove even solution is lowest

Problem 4.

In Chapter ??, the Well Ordering was used to show that all positive rational numbers can be written in "lowest terms," that is, as a ratio of positive integers with no common factor prime factor. Below is a different proof which also arrives at this correct conclusion, but this proof is bogus. Identify every step at which the proof makes an unjustified inference.

Bogus proof. Suppose to the contrary that there was positive rational, q , such that q cannot be written in lowest terms. Now let C be the set of such rational numbers that cannot be written in lowest terms. Then $q \in C$, so C is nonempty. So there must be a smallest rational, $q_0 \in C$. So since $q_0/2 < q_0$, it must be possible to express $q_0/2$ in lowest terms, namely,

$$\frac{q_0}{2} = \frac{m}{n} \quad (3)$$

for positive integers m, n with no common prime factor. Now we consider two cases:

Case 1: [n is odd]. Then $2m$ and n also have no common prime factor, and therefore

$$q_0 = 2 \cdot \left(\frac{m}{n}\right) = \frac{2m}{n}$$

expresses q_0 in lowest terms, a contradiction.

Case 2: [n is even]. Any common prime factor of m and $n/2$ would also be a common prime factor of m and n . Therefore m and $n/2$ have no common prime factor, and so

$$q_0 = \frac{m}{n/2}$$

expresses q_0 in lowest terms, a contradiction.

Since the assumption that C is nonempty leads to a contradiction, it follows that C is empty—that is, there are no counterexamples. ■

Well Ordering Principle

If give any set non empty, non neg \mathbb{N} , there is a minimum value

Used in $\sqrt{2}$ irrational proof

How to prove can express fraction in lowest terms

will be numerator

Can't have prime factor w/ denominator

So can't have common factor

Surprising mileage out of it

But!

- false if set empty

- does set of rational have non negative (?)

$\frac{1}{n}$ for n positive

↳ no least one

- So only works for integers

- negative integers don't count

Use to prove assertions of every non neg integer n

Suppose least \mathbb{N} for which it fails

No such \mathbb{N}

So fails

(2) example
w/ ~~an~~ stack 5¢, 3¢ stamps

Thm: Get any amt $n \geq 8$ ¢

Prove by WOP. Suppose not

m is the least counterexample

↳ can't make, $n \geq 8$ ¢

$m > 8$ $3+5$

$m > 9$ $3+3+3$

$m > 10$ $5+5$

↑ least # can't get

~~Now subtract 3 from it~~

$m \geq 11$

Subtract 3 from

Now $m > 8$

which showed work

Add 3 back

Contradicting the fact

Geometric sums

$$1 + r + r^2 + r^3 + \dots + r^n = \frac{r^{n+1} - 1}{r - 1}$$

Prove holds for every non neg integer $n \geq 0$

Proof by WOP. Let m be smallest n with \neq .

③

When $n=0$ it works

So $m > 0$

Then it will work for $m-1$

(He talks fast - hard to keep up + understand)

So replace n with $m-1$

Smaller than smallest counterexample - so it holds

Prove it works w/ m

Contradiction

Add r^m to both sides

$$1 + r + r^2 + r^3 + \dots + r^{m-1} + r^m = \frac{r^{m+1} - r^m}{r-1}$$

So holds at m

So no counterexample

So true for all non neg integers

Is a standard template

Prove $\forall n \in \mathbb{N}$, $P(n)$ using WOP

Define set of counter examples

$$C := \{n \in \mathbb{N} \mid \text{Not } P(n)\}$$

Assume C is not empty. By WOP have min ele $m \in C$

Then fill in - usually by finding $c \in C$ w/ $c < m$

④ Or any contradiction

Class problems Week 2 Mon

1. ① on sheet

② because you can subtract a

below smallest contradiction

can't be smaller than m - so not part of the contradiction

③ Again must be divisible

(I'm not confusing ② or ③)

④ ~~There must be~~

There is no smallest element in the set

So the set of contradictions must be empty

So must be true

2. (Start w/ template)

~~There must be~~ Define set of counterexamples

Assume must be min element where it is false

Show \emptyset holds, m must be pos, so $m-1$ must hold
anything less than that must hold WOP

(5)

So $0 = 0$

$$0 = \frac{0(1)(1)}{6}$$

$$0 = 0$$

$m-1$ must also hold

Add m^2 to both sides

↳ that $m-1$ step is the same as adding m^2

∴ must also show for $m=1$

$$1 = \frac{1(2)(3)}{6} \quad \text{Q}$$

Or did we get that from the proof

No - don't need to show

But need to add m^2 to both sides

$$\left(\sum_{k=0}^{m-1} k^2 \right) + m^2 = \frac{(m-1)(m)(2m-1)}{6} + m^2$$

? Then show works for 0

No - already showed that 0 satisfies

(People always seem ahead of me!)

6

Board #1

② if $s(m)$ holds, $m = 6x + 15y$

Where x, y are non-neg integers

m is positive $\Rightarrow x \geq 0$ or $y \geq 0$

If $x > 0$, $s(m-6)$ holds: $m-6 = 6(x-1) + 15y \geq 0$

If $y > 0$, $s(m-15)$ holds: $m-15 = 6x + 15(y-1) \geq 0$

③ ~~the~~ m is least counter example

thus $m-6 < m$ is not a counter example

Proof: We did not answer the question required

3. D has to be even

d^4 is also even

$$d^4 = 16d_1^4$$

$$\frac{8a^4 + 4b^4 + 2c^4}{2} = 16d_1^4$$

$$4a^4 + 2b^4 + c^4 = 4d_1^4$$

\uparrow c must be even - sum of even integer

⑦

Repeat for $b + a$

If all even, can factor out 16

- holds - still integers

The least sol is even

$/2 \rightarrow$ still ~~even~~ get a solution

So we did not have the least solution

So there are ~~no~~ no solutions

(Wrote on board)

- agree it's right

- elaborate on why b must be even

4. Responsible for - look at sol after class

Solutions to In-Class Problems Week 2, Mon.

Problem 1.

The proof below uses the Well Ordering Principle to prove that every amount of postage that can be assembled using only 6 cent and 15 cent stamps, is divisible by 3. Let the notation " $j \mid k$ " indicate that integer j is a divisor of integer k , and let $S(n)$ mean that exactly n cents postage can be assembled using only 6 and 15 cent stamps. Then the proof shows that

$$S(n) \text{ IMPLIES } 3 \mid n, \quad \text{for all nonnegative integers } n. \quad (*)$$

Fill in the missing portions (indicated by "...") of the following proof of (*).

Let C be the set of *counterexamples* to (*), namely¹

$$C ::= \{n \mid \dots\}$$

Solution. n is a counterexample to (*) if n cents postage can be made and n is not divisible by 3, so the predicate

$$S(n) \text{ and NOT}(3 \mid n)$$

defines the set, C , of counterexamples. ■

Assume for the purpose of obtaining a contradiction that C is nonempty. Then by the WOP, there is a smallest number, $m \in C$. This m must be positive because...

Solution. ... $3 \mid 0$, so 0 is not a counterexample. ✓ ■

But if $S(m)$ holds and m is positive, then $S(m - 6)$ or $S(m - 15)$ must hold, because...

Solution. ...if $m > 0$ cents postage is made from 6 and 15 cent stamps, at least one stamp must have been used, so removing this stamp will leave another amount of postage that can be made. ■

So suppose $S(m - 6)$ holds. Then $3 \mid (m - 6)$, because...

Solution. ...if NOT($3 \mid (m - 6)$), then $m - 6$ would be a counterexample smaller than m , contradicting the minimality of m . ■

But if $3 \mid (m - 6)$, then obviously $3 \mid m$, contradicting the fact that m is a counterexample.

Next, if $S(m - 15)$ holds, we arrive at a contradiction in the same way. Since we get a contradiction in both cases, we conclude that...

Solution. ... C must be empty. That is, there are no counterexamples to (*), ■

but 3 cents?

which proves that (*) holds.

Problem 2.

Use the Well Ordering Principle to prove that

$$\sum_{k=0}^n k^2 = \frac{n(n+1)(2n+1)}{6}. \quad (1)$$

for all nonnegative integers, n .

Solution. The proof is by contradiction.

Suppose to the contrary that equation (1) failed for some $n \geq 0$. Then by the WOP, there is a *smallest* nonnegative integer, m , such that (1) does not hold when $n = m$.

But (1) clearly holds when $n = 0$, which means that $m \geq 1$. So $m - 1$ is nonnegative, and since it is smaller than m , equation (1) must be true for $n = m - 1$. That is,

$$\sum_{k=0}^{m-1} k^2 = \frac{(m-1)((m-1)+1)(2(m-1)+1)}{6}. \quad (2)$$

Now add $\underline{m^2}$ to both sides of equation (2). Then the left hand side equals

$$\sum_{k=0}^m k^2$$

and the right hand side equals

$$\frac{(m-1)((m-1)+1)(2(m-1)+1)}{6} + m^2$$

Now a little algebra (given below) shows that the right hand side equals

$$\frac{m(m+1)(2m+1)}{6}.$$

That is,

$$\sum_{k=0}^m k^2 = \frac{m(m+1)(2m+1)}{6},$$

contradicting the fact that equation (1) does not hold for m .

It follows that there is no smallest nonnegative integer for which equation (1) fails. Hence (1) must hold for all nonnegative integers.

Here's the algebra:

$$\begin{aligned} \frac{(m-1)((m-1)+1)(2(m-1)+1)}{6} + m^2 &= \frac{(m-1)m(2m-1)}{6} + m^2 \\ &= \frac{(m^2-m)(2m-1)}{6} + m^2 \\ &= \frac{(2m^3-3m^2+m)}{6} + \frac{6m^2}{6} \\ &= \frac{(2m^3+3m^2+m)}{6} \\ &= \frac{m(m+1)(2m+1)}{6} \end{aligned}$$

got this in class
- but why??

Problem 3.

Euler's Conjecture in 1769 was that there are no positive integer solutions to the equation

$$a^4 + b^4 + c^4 = d^4.$$

Integer values for a, b, c, d that do satisfy this equation, were first discovered in 1986. So Euler guessed wrong, but it took more two hundred years to prove it.

Now let's consider Lehman's equation, similar to Euler's but with some coefficients:

$$8a^4 + 4b^4 + 2c^4 = d^4 \quad (3)$$

Prove that Lehman's equation (3) really does not have any positive integer solutions.

Hint: Consider the minimum value of a among all possible solutions to (3).

Solution. Suppose that there exists a solution. Then there must be a solution in which a has the smallest possible value. We will show that, in this solution, $a, b, c,$ and d must all be even. However, we can then obtain another solution over the positive integers with a smaller a by dividing $a, b, c,$ and d in half. This is a contradiction, and so no solution exists.

All that remains is to show that $a, b, c,$ and d must all be even. The left side of Lehman's equation is even, so d^4 is even, so d must be even. Substituting $d = 2d'$ into Lehman's equation gives:

$$8a^4 + 4b^4 + 2c^4 = 16d'^4 \quad \text{how would you know to do that?} \quad (4)$$

Now $2c^4$ must be a multiple of 4, since every other term is a multiple of 4. This implies that c^4 is even and so c is also even. Substituting $c = 2c'$ into the previous equation gives:

$$8a^4 + 4b^4 + 32c'^4 = 16d'^4 \quad (5)$$

Arguing in the same way, $4b^4$ must be a multiple of 8, since every other term is. Therefore, b^4 is even and so b is even. Substituting $b = 2b'$ gives:

$$8a^4 + 64b'^4 + 32c'^4 = 16d'^4 \quad (6)$$

Finally, $8a^4$ must be a multiple of 16, a^4 must be even, and so a must also be even. Therefore, $a, b, c,$ and d must all be even, as claimed. ■

Problem 4.

In Chapter 2, the Well Ordering was used to show that all positive rational numbers can be written in "lowest terms," that is, as a ratio of positive integers with no common factor prime factor. Below is a different proof which also arrives at this correct conclusion, but this proof is bogus. Identify every step at which the proof makes an unjustified inference.

Bogus proof. Suppose to the contrary that there was positive rational, q , such that q cannot be written in lowest terms. Now let C be the set of such rational numbers that cannot be written in lowest terms. Then $q \in C$, so C is nonempty. So there must be a smallest rational, $q_0 \in C$. So since $q_0/2 < q_0$, it must be possible to express $q_0/2$ in lowest terms, namely,

$$\frac{q_0}{2} = \frac{m}{n} \quad (7)$$

for positive integers m, n with no common prime factor. Now we consider two cases:

Case 1: [n is odd]. Then $2m$ and n also have no common prime factor, and therefore

$$q_0 = 2 \cdot \left(\frac{m}{n}\right) = \frac{2m}{n}$$

expresses q_0 in lowest terms, a contradiction.

Case 2: [n is even]. Any common prime factor of m and $n/2$ would also be a common prime factor of m and n . Therefore m and $n/2$ have no common prime factor, and so

$$q_0 = \frac{m}{n/2}$$

expresses q_0 in lowest terms, a contradiction.

Since the assumption that C is nonempty leads to a contradiction, it follows that C is empty—that is, there are no counterexamples. ■

Solution. The proof applies Well Ordering to the positive rationals. Unfortunately, the positive rationals are not Well Ordered, that is, $<$ is not well-founded on the positive rationals. For example, there is no least positive rational. Aside from that, the other steps in the argument are correctly reasoned. ■

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

The Logic of Propositions

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Propositional (Boolean) Logic

A proposition is either True or False

Example:

There are 6 regular solids.

False

Non-examples:

Wake up!

Where am I?

It's 3PM.

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

English to Math

Greeks carry Swords or Javelins

$$G \rightarrow (S \vee J)$$

True even if a Greek carries *both* a Sword and a Javelin

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

English to Math

Greeks carry Bronze or Copper swords

$$G \rightarrow (B \oplus C)$$

Bronze or Copper but not both

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Definition of OR

The value of $(P \text{ OR } Q)$ is T iff P is T, or Q is T, or *both* are T.

Truth Table for OR

P	Q	P OR Q
T	T	T
T	F	T
F	T	T
F	F	F

F iff both P,Q are F

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Definition of AND

The value of $(P \text{ AND } Q)$ is T iff *both* P and Q are T.

Truth Table for AND

P	Q	P AND Q
T	T	T
T	F	F
F	T	F
F	F	F

T iff both P,Q are T

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Definition of NOT

The NOT(P) is T iff P is F.

Truth Table for NOT (P)

P	NOT(P)
T	F
F	T



Albert R Meyer

February 9, 2011

lec 2W.8

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Truth Assignments

A truth assignment assigns a value T or F to each propositional variable. Computer scientists call assignment of values to variables an environment. If we know the environment, we can find the value of a propositional formula.



Albert R Meyer

February 9, 2011

lec 2W.9

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Evaluation in an Environment

Example: Suppose environment, v , assigns $v(P) = T$, $v(Q) = T$, $v(R) = F$.

Truth value of

$(\text{NOT}(P \text{ AND } Q)) \text{ OR } (R \text{ XOR NOT}(Q))$

F T T T F F F F T



Albert R Meyer

February 9, 2011

lec 2W.11

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Equivalence

Two propositional formulas are equivalent iff they have the same truth value in all environments.



Albert R Meyer

February 9, 2011

lec 2W.12

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

DeMorgan's Law

$P \vee Q$ is equivalent to $\overline{\overline{P} \wedge \overline{Q}}$

P	Q	$\overline{(P \vee Q)}$
T	T	F
T	F	F
F	T	F
F	F	T

$\overline{\overline{P} \wedge \overline{Q}}$
F
F
F
T
T



Albert R Meyer

February 9, 2011

lec 2W.14

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

DeMorgan's Law

$P \vee Q$ is equivalent to $\overline{\overline{P} \wedge \overline{Q}}$

P	Q	$\overline{(P \vee Q)}$
T	T	F
T	F	F
F	T	F
F	F	T

$\overline{\overline{P} \wedge \overline{Q}}$
F
F
F
T
T


Same final column, so equivalent -- proof by Truth Table



Albert R Meyer

February 9, 2011

lec 2W.15


 **Definition of IMPLIES**


The value of (P IMPLIES Q) is F iff P is T and Q is F.

Truth Table for IMPLIES (\rightarrow)


P	Q	$P \rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T


F iff P is T
Q is F

 Albert R Meyer February 9, 2011 lec 2W.16


 **A True Implication**


($1=-1$) IMPLIES (I am Pope)
We reasoned *correctly* to reach the false conclusion

 Albert R Meyer February 9, 2011 lec 2W.17


 **A True Implication**


($1=-1$) IMPLIES (I am Pope)
We reasoned *correctly* to reach the false conclusion

 Albert R Meyer February 9, 2011 lec 2W.18


 **A True Implication**


($1=-1$) IMPLIES (I am Pope)
We reasoned *correctly* to reach the false conclusion from the false hypothesis.

 Albert R Meyer February 9, 2011 lec 2W.19


 **A True Implication**

($1=-1$) IMPLIES (I am Pope)
We reasoned *correctly* to reach the false conclusion from the false hypothesis.

 Albert R Meyer February 9, 2011 lec 2W.20

 **A True Implication**

($1=-1$) IMPLIES (I am Pope)
The *whole implication is true*, even though both conclusion & hypothesis are false.

 Albert R Meyer February 9, 2011 lec 2W.21

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Satisfiability & Validity

A formula is satisfiable iff it is true in some environment.

A formula is valid iff it is true in all environments.



Albert R. Meyer

February 9, 2011

lec 2W.22

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Verifying Valid, Satisfiable

Truth table size doubles with each additional variable
 --exponential growth. Makes truth tables impossible when there are hundreds of variables. (In current digital circuits, there are millions of variables.)



Albert R. Meyer

February 9, 2011

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Efficient Test for Satisfiability?

The P=NP? question is equivalent to asking if there is an efficient (polynomial rather than exponential time) procedure to check satisfiability.



Albert R. Meyer

February 9, 2011

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Other Applications

Java Logical Expressions:

```

OR      AND
if ((x>0) || (x <= 0 && y>100))
    :
    (more code)
  
```



Albert R. Meyer

February 9, 2011

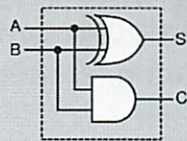
lec 2W.39

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Application: Digital Logic

$$s ::= A \text{ XOR } B$$

$$c ::= A \text{ AND } B$$



half adder



Albert R. Meyer

February 9, 2011

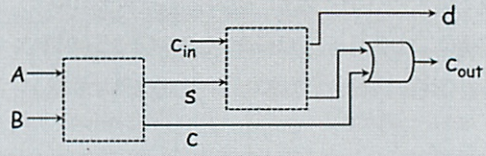
lec 2W.41

6	9	13	7
12	10	5	
3	1	4	14
15	8	11	2

Digital Logic

$$d ::= c_{in} \text{ XOR } s$$

$$c_{out} ::= (c_{in} \text{ AND } s) \text{ OR } c$$



full adder



Albert R. Meyer

February 9, 2011

lec 2W.42

6	9	13	7
12		10	5
3	1	4	14
15	8	11	2

Team Problems

Problems

1-4



Albert R. Meyer

February 9, 2011

lec 2W.43

Propositions - either true or false
invariant
can be determined

Math to combine ~~propositioned~~ propositions
- pin down language

Implies \rightarrow

Or \vee

- not exclusive
- can be both!

XOR

~~- must be both~~

one or the other
but not both

\oplus

look at
truth tables

AND - both

NOT - inverts

assignments / environments

- we can write little program to make truth tables

②

~~Just~~ Write the long string
and what values we have

1. Reduce NOTs
2. " XORs and ANDs
3. " ORs

Recursively to higher level
(did in ~~the~~ 6.01)

Equivalence - means same thing

De Morgan $\overline{P \vee Q} = \overline{P} \wedge \overline{Q}$ ^{← NOT}

check w/ truth table

→ also means not

Implies

'is F iff P is T and Q is F

↳ for P IMPLIES Q

~~↳ same as Q IF P~~

not same as philosophy implies

(3)

Satisfiable iff it is true in some environment

Valid if it is always true

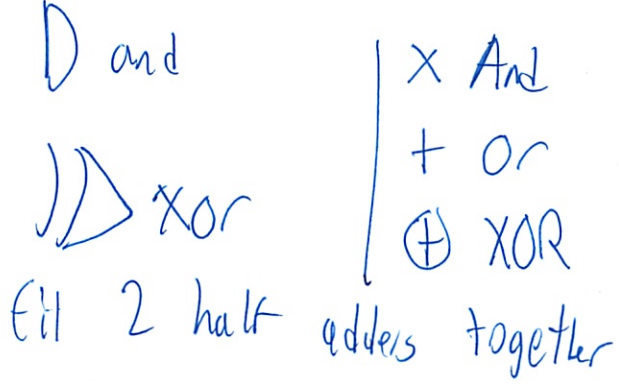
Verifying Valid, Satisfiability is a big problem

- truth table increases at 2^n
- exponential
- we don't know any other general theorem
- the P=NP question
- core unsolved theoretical problem

Conditional tests in Java

Digital logic

- how circuits are constructed



In-Class Problems Week 2, Wed.

Problem 1.

Prove by truth table that OR distributes over AND, namely,

$$P \text{ OR } (Q \text{ AND } R) \text{ is equivalent to } (P \text{ OR } Q) \text{ AND } (P \text{ OR } R) \quad (1)$$

Problem 2.

This problem¹ examines whether the following specifications are *satisfiable*:

1. If the file system is not locked, then
 - (a) new messages will be queued.
 - (b) new messages will be sent to the messages buffer.
 - (c) the system is functioning normally, and conversely, if the system is functioning normally, then the file system is not locked.
2. If new messages are not queued, then they will be sent to the messages buffer.
3. New messages will not be sent to the message buffer.

(a) Begin by translating the five specifications into propositional formulas using four propositional variables:

$L ::=$ file system locked,
 $Q ::=$ new messages are queued,
 $B ::=$ new messages are sent to the message buffer,
 $N ::=$ system functioning normally.

(b) Demonstrate that this set of specifications is satisfiable by describing a single truth assignment for the variables L , Q , B , N and verifying that under this assignment, all the specifications are true.

(c) Argue that the assignment determined in part (b) is the only one that does the job.


Problem 3.

When the mathematician says to his student, "If a function is not continuous, then it is not differentiable," then letting D stand for "differentiable" and C for continuous, the only proper translation of the mathematician's statement would be

$$\text{NOT}(C) \text{ IMPLIES } \text{NOT}(D),$$

or equivalently,

$$D \text{ IMPLIES } C.$$

Creative Commons  2011, Eric Lehman, F Tom Leighton, Albert R Meyer .

¹From Rosen, 5th edition, Exercise 1.1.36

$\neg = \neg$ not same notation

But when a mother says to her son, "If you don't do your homework, then you can't watch TV," then letting T stand for "watch TV" and H for "do your homework," a reasonable translation of the mother's statement would be

$$\text{NOT}(H) \text{ IFF } \text{NOT}(T),$$

or equivalently,

$$H \text{ IFF } T.$$

Explain why it is reasonable to translate these two IF-THEN statements in different ways into propositional formulas.

Problem 4.

Propositional logic comes up in digital circuit design using the convention that **T** corresponds to 1 and **F** to 0. A simple example is a 2-bit *half-adder* circuit. This circuit has 3 binary inputs, a_1, a_0 and b , and 3 binary outputs, c, o_1, o_0 . The 2-bit word a_1a_0 gives the binary representation of an integer, k , between 0 and 3. The 3-bit word cs_1s_0 gives the binary representation of $k + b$. The third output bit, c , is called the final *carry bit*.

So if k and b were both 1, then the value of a_1a_0 would be 01 and the value of the output cs_1s_0 would 010, namely, the 3-bit binary representation of $1 + 1$.

In fact, the final carry bit equals 1 only when all three binary inputs are 1, that is, when $k = 3$ and $b = 1$. In that case, the value of cs_1s_0 is 100, namely, the binary representation of $3 + 1$.

This 2-bit half-adder could be described by the following formulas:

$$c_0 = b$$

$$s_0 = a_0 \text{ XOR } c_0$$

$$c_1 = a_0 \text{ AND } c_0$$

$$s_1 = a_1 \text{ XOR } c_1$$

$$c_2 = a_1 \text{ AND } c_1$$

$$c = c_2.$$

the carry into column 1

the carry into column 2

S and 0 same
- typo

(a) Generalize the above construction of a 2-bit half-adder to an $n+1$ bit half-adder with inputs a_n, \dots, a_1, a_0 and b for arbitrary $n \geq 0$. That is, give simple formulas for s_i and c_i for $0 \leq i \leq n+1$, where c_i is the carry into column i and $c = c_{n+1}$.

(b) Write similar definitions for the digits and carries in the sum of two $n+1$ -bit binary numbers $a_n \dots a_1 a_0$ and $b_n \dots b_1 b_0$.

Visualized as digital circuits, the above adders consist of a sequence of single-digit half-adders or adders strung together in series. These circuits mimic ordinary pencil-and-paper addition, where a carry into a column is calculated directly from the carry into the previous column, and the carries have to ripple across all the columns before the carry into the final column is determined. Circuits with this design are called *ripple-carry* adders. Ripple-carry adders are easy to understand and remember and require a nearly minimal number of operations. But the higher-order output bits and the final carry take time proportional to n to reach their final values.

(c) How many of each of the propositional operations does your adder from part (b) use to calculate the sum?

The Propositional Operations

P	NOT P
T	F
F	T

P	Q	P AND Q
T	T	T
T	F	F
F	T	F
F	F	F

P	Q	P OR Q
T	T	T
T	F	T
F	T	T
F	F	F

P	Q	P XOR Q
T	T	F
T	F	T
F	T	T
F	F	F

P	Q	P IMPLIES Q
T	T	T
T	F	F
F	T	T
F	F	T

P	Q	P IFF Q
T	T	T
T	F	F
F	T	F
F	F	T

④ (one I can actually do! yay) - deterministic solution

$$P \text{ or } (Q \text{ and } R) = (P \text{ or } Q) \text{ And } (P \text{ or } R)$$

2^3 rows = 8

P	Q	R
T	T	T
T	T	F
T	F	T
F	T	T
F	T	F
F	F	F
T	F	F
F	F	T

P	Q And R	OR
	T	T
	F	T
	F	T
	T	T
	F	F
	F	F
	F	T
	F	F

P Or Q	P Or R	And
T	T	T
T	T	T
T	T	T
T	T	T
T	F	F
F	F	F
T	T	T
F	T	F

done (✓) matches

⑤ 2. Satisfiable - true ~~can~~ sometimes

L = locked

Q = queued

B = buffer

N = functioning normally

(another ~~very~~ challenging + double \rightarrow fun problems)

$$\begin{array}{l} \bar{L} \text{ implies } Q \\ \bar{L} \rightarrow B \end{array} \quad) \quad \bar{L} \rightarrow (Q \wedge B)$$

$$\begin{array}{l} \bar{L} \rightarrow N \\ N \rightarrow \bar{L} \end{array} \quad) \quad \text{converse same as IFF} \downarrow$$

$$\begin{array}{l} \bar{L} \text{ IFF } N \\ \bar{L} \Leftrightarrow N \end{array}$$

$$\bar{Q} \rightarrow B$$

\bar{B} \leftarrow can just write that in here

b) Find a single way of saying this

Review $\bar{L} \rightarrow (Q \wedge B)$ $\bar{Q} \rightarrow B$

~~$\bar{L} \rightarrow B$~~ duplicate

$$\bar{L} \Leftrightarrow N$$

\bar{B}
 \leftarrow start from

6

\bar{B}

$$\bar{L} \rightarrow (Q \wedge B)$$

$$\bar{Q} \rightarrow B \quad \text{so} \quad \bar{B} \rightarrow Q$$

contrapositive
double negation

Q must be true

$$\bar{L} \rightarrow B \quad \text{so} \quad \bar{B} \rightarrow L$$

Contrapositive

L must be true

$$\bar{L} \leftrightarrow N \quad \text{so} \quad \bar{N} \leftrightarrow L$$

↗ equivalent-ish

$$\bar{B} \rightarrow Q \wedge L \wedge \bar{N}$$

∧ = and

∧ this is it

~~$\bar{B} \rightarrow Q \wedge L \wedge \bar{N}$~~

$$\bar{B} \wedge Q \wedge L \wedge \bar{N}$$

7

c) Everything is specified

~~B~~ B must be false

"an assignment"

$\bar{Q} \rightarrow B$ so $\bar{B} \rightarrow Q$

e said true here

Q is false true

$\bar{L} \rightarrow B$ so $\bar{B} \rightarrow L$

L must be true

$\bar{L} \leftrightarrow N$ so N must be false

(just a rewrite of above)

3.

~~C~~ $\bar{C} \rightarrow \bar{D}$

$D \rightarrow C$ contrapositive

differentiable implies continuous

~~H~~ $H \leftrightarrow \bar{T}$

~~H~~

$H \leftrightarrow T$

You can only do your hw if and only if you watch TV

8

Just say that math is more precise

TV is optional

~~if~~ $H \rightarrow T$

If you do your HW, you can watch TV

If you do not do your HW you can not TV

$\text{Not}(H) \rightarrow \text{Not}(T)$

Contra pos

$T \rightarrow H$ is wrong

$H \rightarrow T$

$\text{Not}(T) \rightarrow \text{Not}(H)$

Not watching TV means you can not do your HW

↳ don't want that either

So how would you write this?

H	T	
T	T	✓
T	F	✓
F	T	x
F	F	x

Oh time based
HW must be first

9

H is the statement

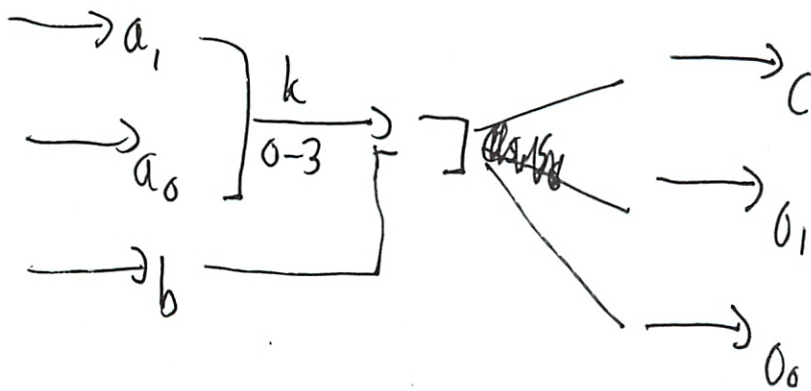
↳ t does not matter

~~Answer~~

4.

half-adder

↳ from word description
prob horribly wrong



k	b	a_1, a_0	c, o_1, o_0
1	1	01	010
3	1		100

What is the final carry bit?

10

(Need a better description of half adder)

$$C_0 = b$$

$$S_0 = a_0 \oplus C_0$$

$$C_1 = a_0 \times C_0$$

$$S_1 = a_1 \oplus C_1$$

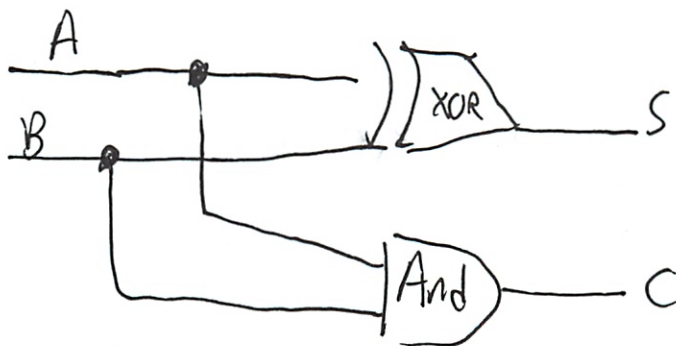
$$C_2 = a_1 \times C_1$$

$$C = C_2$$

Now generalize to $n+1$ half adder

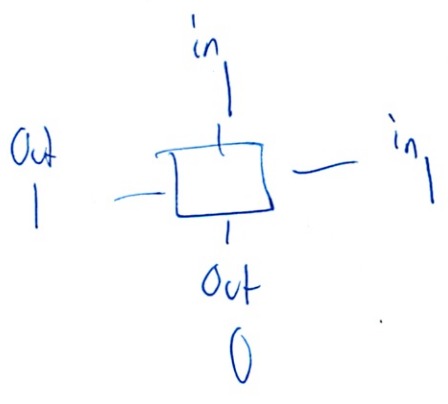
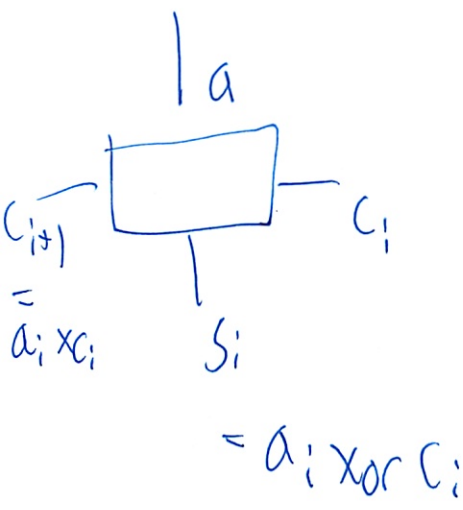
-(I don't even understand a regular half adder!)

Wikipedia



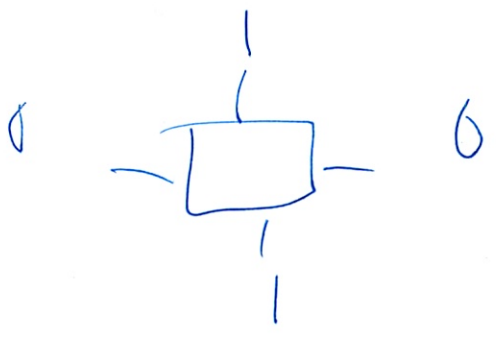
$2C + S$

11



in 1 + 1

out 2



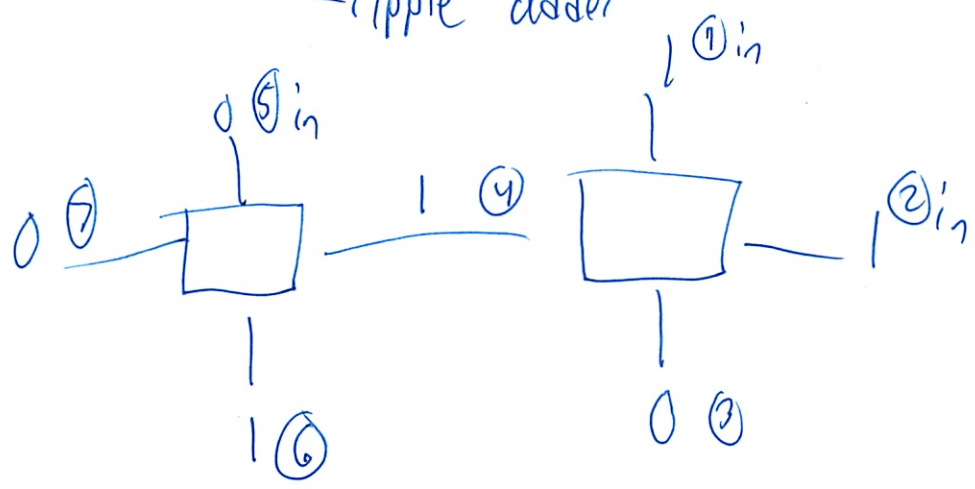
in 1 + 0

out 1

(7)

Hook together

- ripple adder

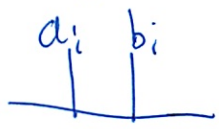


in 1+1

Out is 2

keep hooking together

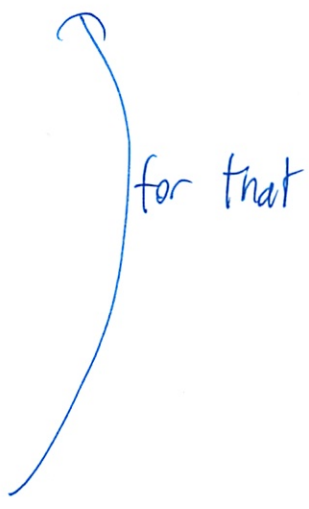
final adder takes



← notation

adding 2 binary # bits

hook up a bunch together



Solutions to In-Class Problems Week 2, Wed.

Problem 1.

Prove by truth table that OR distributes over AND, namely,

$$P \text{ OR } (Q \text{ AND } R) \text{ is equivalent to } (P \text{ OR } Q) \text{ AND } (P \text{ OR } R) \quad (1)$$

Solution.

P	Q	R	$P \text{ OR } (Q \text{ AND } R)$	$(P \text{ OR } Q) \text{ AND } (P \text{ OR } R)$
T	T	T	T	T
T	T	F	T	T
T	F	T	T	T
T	F	F	T	T
F	T	T	T	T
F	T	F	F	F
F	F	T	F	F
F	F	F	F	F

The highlighted column giving the truth values of the first formula is the same as the corresponding column of the second formula, so the two propositional formulas are equivalent. ■

Problem 2.

This problem¹ examines whether the following specifications are *satisfiable*:

1. If the file system is not locked, then
 - (a) new messages will be queued.
 - (b) new messages will be sent to the messages buffer.
 - (c) the system is functioning normally, and conversely, if the system is functioning normally, then the file system is not locked.
2. If new messages are not queued, then they will be sent to the messages buffer.
3. New messages will not be sent to the message buffer.

(a) Begin by translating the five specifications into propositional formulas using four propositional variables:

$L ::=$ file system locked,
 $Q ::=$ new messages are queued,
 $B ::=$ new messages are sent to the message buffer,
 $N ::=$ system functioning normally.

Solution. The translations of the specifications are:

$\text{NOT}(L) \text{ IMPLIES } Q$	(Spec. 1.(a))
$\text{NOT}(L) \text{ IMPLIES } B$	(Spec. 1.(b))
$\text{NOT}(L) \text{ IFF } N$	(Spec. 1.(c))
$\text{NOT}(Q) \text{ IMPLIES } B$	(Spec. 2.)
$\text{NOT}(B)$	(Spec. 3.)

■

(b) Demonstrate that this set of specifications is satisfiable by describing a single truth assignment for the variables L , Q , B , N and verifying that under this assignment, all the specifications are true.

Solution. An assignment that works is

$L = \mathbf{T}$
 $N = \mathbf{F}$
 $Q = \mathbf{T}$
 $B = \mathbf{F}$.

To find this assignment, we could have started constructing the sixteen line truth table—one line for each way of assigning truth values to the four variables L , N , Q , and B —and calculated the truth value of the AND of all the five specifications under that assignment, continuing until we got one that made the AND-formula true.

If for every one of the sixteen possible truth assignments, the AND-formula was false, then the system is not satisfiable. ■

¹From Rosen, 5th edition, Exercise 1.1.36

(c) Argue that the assignment determined in part (b) is the only one that does the job.

Solution. We can avoid calculating all 16 rows of the full truth table calculation suggested in the solution to part (b) by reasoning as follows. In any truth assignment that makes all five specifications true,

- B must be false, or the last specification, (Spec. 3.), would be false.
- Given that B is false, (Spec. 2.) and (Spec. 1.(b)) can be true only if Q and L are true.
- Given that L is true, (Spec. 1.(c)) can be true only if N is false.

Thus, in order for all five specifications to be true, the assignment has to be the one in the solution to part (b) ■

Problem 3.

When the mathematician says to his student, “If a function is not continuous, then it is not differentiable,” then letting D stand for “differentiable” and C for continuous, the only proper translation of the mathematician’s statement would be

$$\text{NOT}(C) \text{ IMPLIES } \text{NOT}(D),$$

or equivalently,

$$D \text{ IMPLIES } C.$$

But when a mother says to her son, “If you don’t do your homework, then you can’t watch TV,” then letting T stand for “watch TV” and H for “do your homework,” a reasonable translation of the mother’s statement would be

$$\text{NOT}(H) \text{ IFF } \text{NOT}(T),$$

or equivalently,

$$H \text{ IFF } T.$$

Explain why it is reasonable to translate these two IF-THEN statements in different ways into propositional formulas.

Solution. We know that a differentiable function must be continuous, so when a function is not continuous, it is also not differentiable. Now mathematicians use IMPLIES in the technical way given by its truth table. In particular, if a function *is* continuous then to a mathematician, the implication

$$\text{NOT}(C) \text{ IMPLIES } \text{NOT}(D),$$

is automatically true since the hypothesis (left hand side of the IMPLIES) is false. So whether or not continuity holds, the mathematician could comfortably assert the IMPLIES statement knowing it is correct.

And of course a mathematician does *not* mean IFF, since she knows a function that is not differentiable may well be continuous.

On the other hand, while the mother certainly means that her son cannot watch TV if he does not do his homework, both she and her son *most likely* understand that if he *does* do his homework, then he *will* be allowed watch TV. In this case, even though the Mother uses an IF-THEN phrasing, she really means IFF.

On the other hand, circumstances in the household might be that the boy may watch TV when he has not only done his homework, but *also* cleaned up his room. In this case, just doing homework would not imply being allowed to watch TV—the boy won’t be allowed to watch TV if he hasn’t cleaned his room, even if he has done his homework.

The general point here is that semantics (meaning) trumps syntax (sentence structure): even though the mathematician’s and mother’s statements have the same structure, their meaning may warrant different translations into precise logical language. ■

but no nice way to show Mom's meaning

Problem 4.

Propositional logic comes up in digital circuit design using the convention that **T** corresponds to 1 and **F** to 0. A simple example is a 2-bit *half-adder* circuit. This circuit has 3 binary inputs, a_1, a_0 and b , and 3 binary outputs, c, s_1, s_0 . The 2-bit word a_1a_0 gives the binary representation of an integer, k , between 0 and 3. The 3-bit word cs_1s_0 gives the binary representation of $k + b$. The third output bit, c , is called the final *carry bit*.

So if k and b were both 1, then the value of a_1a_0 would be 01 and the value of the output cs_1s_0 would 010, namely, the 3-bit binary representation of $1 + 1$.

In fact, the final carry bit equals 1 only when all three binary inputs are 1, that is, when $k = 3$ and $b = 1$. In that case, the value of cs_1s_0 is 100, namely, the binary representation of $3 + 1$.

This 2-bit half-adder could be described by the following formulas:

$$\begin{aligned} c_0 &= b \\ s_0 &= a_0 \text{ XOR } c_0 \\ c_1 &= a_0 \text{ AND } c_0 && \text{the carry into column 1} \\ s_1 &= a_1 \text{ XOR } c_1 \\ c_2 &= a_1 \text{ AND } c_1 && \text{the carry into column 2} \\ c &= c_2. \end{aligned}$$

(a) Generalize the above construction of a 2-bit half-adder to an $n+1$ bit half-adder with inputs a_n, \dots, a_1, a_0 and b for arbitrary $n \geq 0$. That is, give simple formulas for s_i and c_i for $0 \leq i \leq n+1$, where c_i is the carry into column i and $c = c_{n+1}$.

Solution. The $n+1$ -bit word $a_n \dots a_1 a_0$ will be the binary representation of an integer, s , between 0 and $2^{n+1} - 1$. The circuit will have $n+2$ outputs c, s_n, \dots, s_1, s_0 where the $n+2$ -bit word $cs_n \dots s_1 s_0$ gives the binary representation of $s + b$.

Here are some simple formulas that define such a half-adder:

$$\begin{aligned} c_0 &= b, \\ s_i &= a_i \text{ XOR } c_i && \text{for } 0 \leq i \leq n, \\ c_{i+1} &= a_i \text{ AND } c_i && \text{for } 0 \leq i \leq n, \\ c &= c_{n+1}. \end{aligned}$$

■

(b) Write similar definitions for the digits and carries in the sum of two $n+1$ -bit binary numbers $a_n \dots a_1 a_0$ and $b_n \dots b_1 b_0$.

Solution. Define

$$\begin{aligned} c_0 &= 0 \\ s_i &= a_i \text{ XOR } b_i \text{ XOR } c_i && \text{for } 0 \leq i \leq n, \\ c_{i+1} &= (a_i \text{ AND } b_i) \text{ OR} \\ &\quad (a_i \text{ AND } c_i) \text{ OR } (b_i \text{ AND } c_i) && \text{for } 0 \leq i \leq n, \\ c &= c_{n+1}. \end{aligned}$$

■

Visualized as digital circuits, the above adders consist of a sequence of single-digit half-adders or adders strung together in series. These circuits mimic ordinary pencil-and-paper addition, where a carry into a column is calculated directly from the carry into the previous column, and the carries have to ripple across all the columns before the carry into the final column is determined. Circuits with this design are called *ripple-carry* adders. Ripple-carry adders are easy to understand and remember and require a nearly minimal number of operations. But the higher-order output bits and the final carry take time proportional to n to reach their final values.

(c) How many of each of the propositional operations does your adder from part (b) use to calculate the sum?

Solution. The scheme given in the solution to part (b) uses $3(n + 1)$ AND's, $2(n + 1)$ XOR's, and $2(n + 1)$ OR's for a total of $7(n + 1)$ operations.²



The Propositional Operations

P	NOT P
T	F
F	T

P	Q	P AND Q
T	T	T
T	F	F
F	T	F
F	F	F

P	Q	P OR Q
T	T	T
T	F	T
F	T	T
F	F	F

P	Q	P XOR Q
T	T	F
T	F	T
F	T	T
F	F	F

P	Q	P IMPLIES Q
T	T	T
T	F	F
F	T	T
F	F	T

P	Q	P IFF Q
T	T	T
T	F	F
F	T	F
F	F	T

²Because c_0 is always 0, you could skip all the operations involving it. Then the counts are $3n + 1$ AND's, $2n + 1$ XOR's, and $2n$ OR's for a total of $7n + 2$ operations.