

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

Mathematics for Computer Science 6.042J/18.062J

WELCOME!

Prof. Albert R. Meyer

<http://theory.lcs.mit.edu/classes/6.042>

“Proof, Proofs & More Proofs”

Copyright © Albert R. Meyer, 2007. All rights reserved. Feb. 7, 2006

lec 1W.1

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

Quick Summary

1. Fundamental Concepts of Discrete Mathematics.
2. Discrete Mathematical Structures
(like *trees* or *lists*)
3. Discrete Probability Theory.

Copyright © Albert R. Meyer, 2007. All rights reserved. Feb. 7, 2006

lec 1W.2

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

Vocabulary

Quickie:

What does “discrete” mean?
(≠ “discreet”)

Copyright © Albert R. Meyer, 2007. All rights reserved. Feb. 7, 2006

lec 1W.3

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

Online Tutor Problems 1

Due Friday, 6pm:
Part 1.1: Course Registration

Due Monday, 6pm:
Part 1.2: Diagnostic Questionnaire

Copyright © Albert R. Meyer, 2007. All rights reserved. Feb. 7, 2006

lec 1W.4

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

Reading Assignment

Reading: Notes for week 1;
Week 2 also available
(see course calendar)

Email comments on **week 1&2** Notes:
due next Wednesday, 11am

Copyright © Albert R. Meyer, 2007. All rights reserved. Feb. 7, 2006

lec 1W.5

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

Course Organization

- **Web site:** All course handouts.
- **Problem Sets:** *up to 30%* of grade (see **course info**).

Copyright © Albert R. Meyer, 2007. All rights reserved. Feb. 7, 2006

lec 1W.6

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

Course Organization

- **Studio-Lecture Style:**
mix of mini-lectures &
team problem-solving;
preparation & attendance
required (25% of grade)

Copyright © Albert R. Meyer, 2007. All rights reserved. Feb. 7, 2006

lec 1W.7

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 .

Copyright © Albert R. Meyer, 2007. All rights reserved. Feb. 7, 2006

lec 1W.8

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

Active Lectures

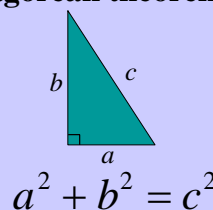
Quickie question:
Where was your neighbor
born?

Copyright © Albert R. Meyer, 2007. All rights reserved. Feb. 7, 2006

lec 1W.9

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

Getting started: Pythagorean theorem



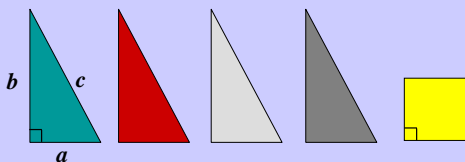
Familiar? Yes!
Obvious? No!

Copyright © Albert R. Meyer, 2007. All rights reserved. Feb. 7, 2006

lec 1W.10

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

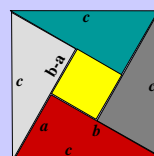
(Many many proofs: <http://www.cut-the-knot.com>)

Copyright © Albert R. Meyer, 2007. All rights reserved. Feb. 7, 2006

lec 1W.11

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

A Cool Proof



Copyright © Albert R. Meyer, 2007. All rights reserved. Feb. 7, 2006

lec 1W.12

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

A Cool Proof

Copyright © Albert R. Meyer, 2007 All rights reserved. Feb. 7, 2006 lec 1W.13

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

A Cool Proof

Copyright © Albert R. Meyer, 2007 All rights reserved. Feb. 7, 2006 lec 1W.14

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

A False Proof: Getting Rich By Diagram

Copyright © Albert R. Meyer, 2007 All rights reserved. Feb. 7, 2006 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

Copyright © Albert R. Meyer, 2007 All rights reserved. Feb. 7, 2006 lec 1W.16

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

Getting Rich

The bug:

are not right triangles!

The top and bottom line of the “rectangle” is not straight!

Copyright © Albert R. Meyer, 2007 All rights reserved. Feb. 7, 2006 lec 1W.17

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

Another False Proof

Theorem:

Every polynomial, $ax^2 + bx + c$, has two roots over \mathbb{C} .

Proof (by calculation):

The polynomial $ax^2 + bx + c$ has roots

$$r_1 = \frac{-b + \sqrt{b^2 - 4ac}}{2a} \quad \text{and} \quad r_2 = \frac{-b - \sqrt{b^2 - 4ac}}{2a}$$

Copyright © Albert R. Meyer, 2007 All rights reserved. Feb. 7, 2006 lec 1W.18

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

Another False proof

Counter-examples:

$0x^2 + 0x + 1$ has 0 roots.

$0x^2 + 1x + 1$ has 1 root.

The bug: divide by zero error.

The fix: assume $a \neq 0$.

Copyright © Albert R. Meyer, 2007 All rights reserved. Feb. 7, 2006

lec 1W.19

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

Another false proof

Counter-example:

$1x^2 + 0x + 0$ has 1 root.

The bug: $r_1 = r_2$

The fix: need hypothesis $D \neq 0$ where

$$D ::= \sqrt{b^2 - 4ac}$$

Copyright © Albert R. Meyer, 2007 All rights reserved. Feb. 7, 2006

lec 1W.20

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

Another false proof

Ambiguity when $D < 0$:

$x^2 + 1$ has roots $i, -i$.

Which is r_1 , which is r_2 ?

Copyright © Albert R. Meyer, 2007 All rights reserved. Feb. 7, 2006

lec 1W.21

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

$1 = -1$?

The ambiguity causes problems:

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

Moral: “mindless” calculation not safe.

1. Be sure rules are properly applied.
2. Calculation is a risky substitute for understanding.

Copyright © Albert R. Meyer, 2007 All rights reserved. Feb. 7, 2006

lec 1W.22

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

Consequences of $1 = -1$

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

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

“Since 1 and the Pope are clearly 2,
we conclude that

1 and the Pope are 1.

That is, I am the Pope.”

-- Bertrand Russell

Copyright © Albert R. Meyer, 2007 All rights reserved. Feb. 7, 2006

lec 1W.23

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: <http://www.uneca.drexel.edu/~jlane/brs.html>)

Copyright © Albert R. Meyer, 2007 All rights reserved. Feb. 7, 2006

lec 1W.24

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

In-class Problems

PROBLEMS 1 & 2

Copyright © Albert R. Meyer, 2007. All rights reserved.

Feb. 7, 2006

lec 1W.25

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

Mathematics for Computer Science

MIT 6.042J/18.062J

Truth & Proof

Math vs. Reality
Propositional Logic

Copyright © Albert R. Meyer, 2007. All rights reserved. February 9, 2007

lec 1F.1

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

Team Problem

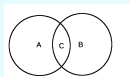
Surprise Problem 1

Copyright © Albert R. Meyer, 2007. All rights reserved. February 9, 2007

lec 1F.2

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

Math



Sets

Numbers $4, \sqrt{7}, \pi, i + 1$

T, F

Booleans

Strings

"albert meyer"

$$f(x) ::= x^2 + 2$$

Functions

Relations

$$a \leq b$$



Data structures

Copyright © Albert R. Meyer, 2007. All rights reserved. February 9, 2007

lec 1F.3

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

Not Math



Family

Copyright © Albert R. Meyer, 2007. All rights reserved. February 9, 2007

lec 1F.4

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

Not Math



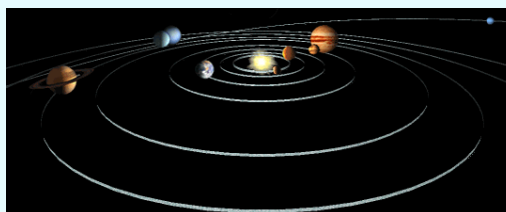
Cats

Copyright © Albert R. Meyer, 2007. All rights reserved. February 9, 2007

lec 1F.5

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

Not Math



Solar System

Copyright © Albert R. Meyer, 2007. All rights reserved. February 9, 2007

lec 1F.6

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

Not Math: Cogito ergo sum



René Descartes'
MEDITATIONS

on First Philosophy in which the *Existence of God* and
the Distinction Between Mind and Body are Demonstrated.

(Picture source: <http://www.brinternet.com/~glynhughes/eqsahed/descartes.html>)
Copyright © Albert R. Meyer, 2007. All rights reserved. February 9, 2007

lec 1F.7

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

Evidence vs. Proof

Let $p(n) ::= n^2 + n + 41$.

Claim:

$\forall n \in \mathbb{N}$. $p(n)$ is a prime number
for all n that are *nonnegative integers*

Copyright © Albert R. Meyer, 2007. All rights reserved. February 9, 2007

lec 1F.8

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

Only Prime Numbers?

Evidence:

$p(0) = 41$	prime	
$p(1) = 43$	prime	
$p(2) = 47$	prime	
$p(3) = 53$	prime	
\vdots		
$p(20) = 461$	prime	looking good!
\vdots		
$p(39) = 1601$	prime	enough already!

Copyright © Albert R. Meyer, 2007. All rights reserved. February 9, 2007

lec 1F.9

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

Only Prime Numbers?

$\forall n \in \mathbb{N}$. $p(n) ::= n^2 + n + 41$
is a prime number

This is not a coincidence.
The hypothesis must be true. *But no!*

$p(40) = 1681$ is *not prime*.

Copyright © Albert R. Meyer, 2007. All rights reserved. February 9, 2007

lec 1F.10

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

Only Prime Numbers?

Quickie:

Prove that **1681** is not prime.

Proof: $1681 = p(40)$
 $= 40^2 + 40 + 41$
 $= 40^2 + 2 \cdot 40 + 1$
 $= (40 + 1)^2$

Copyright © Albert R. Meyer, 2007. All rights reserved. February 9, 2007

lec 1F.11

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

Further Extreme Example

Hypothesis:

$$313 \cdot (x^3 + y^3) = z^3$$

has no solution in positive integers

False. But smallest counterexample
has more than 1000 digits!

Copyright © Albert R. Meyer, 2007. All rights reserved. February 9, 2007

lec 1F.14

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

P = NP?

- Overwhelming evidence for \neq based on centuries of experience
- Modern cryptography (like RSA) depends on \neq
- Nearly all experts believe \neq
- But *mathematically unproven* – the most important open problem in CS

Copyright © Albert R. Meyer, 2007. All rights reserved. February 9, 2007

lec 1F.15

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

Propositional (Boolean) Logic

Proposition is either **True** or **False**

Examples: $2 + 2 = 4$ **True**
 $1 \times 1 = 4$ **False**

Non-examples: Wake up!
Where am I?

Copyright © Albert R. Meyer, 2007. All rights reserved. February 9, 2007

lec 1F.19

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

Operators

$\wedge ::=$ AND
 $\vee ::=$ OR
 $\neg ::=$ NOT
 $\rightarrow ::=$ IMPLIES (if ... then)
 $\leftrightarrow ::=$ IFF (if and only if)

Copyright © Albert R. Meyer, 2007. All rights reserved. February 9, 2007

lec 1F.20

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

English to Math

“If Greeks are Human, and Humans are Mortal, then Greeks are Mortal.”

$((G \rightarrow H) \wedge (H \rightarrow M)) \rightarrow (G \rightarrow M)$

Copyright © Albert R. Meyer, 2007. All rights reserved. February 9, 2007

lec 1F.21

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

English to Math

Greeks carry Swords or Javelins

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

True even if a Greek carries both

Copyright © Albert R. Meyer, 2007. All rights reserved. February 9, 2007

lec 1F.22

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

English to Math

Greeks carry Bronze or Flint swords

$(G \rightarrow B) \oplus (G \rightarrow F)$
⏟
exclusive-or

$P \oplus Q$ means “ P or Q but **not both**”

Copyright © Albert R. Meyer, 2007. All rights reserved. February 9, 2007

lec 1F.23

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

Math vs. English

Parent: If you don't clean your room,
you can't watch a DVD."

$$\neg C \longrightarrow \neg D$$

$$C \longrightarrow D \quad ? \text{ YES!}$$

Copyright © Albert R. Meyer, 2007. All rights reserved. February 9, 2007

lec 1F.24

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

Math vs. English

Parent: If you don't clean your room,
you can't watch a DVD."

that is

$$C \longleftrightarrow D$$

Copyright © Albert R. Meyer, 2007. All rights reserved. February 9, 2007

lec 1F.25

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

Math vs. English

Mathematician:
"If a function is not continuous,
then it is not differentiable."

$$\neg C \longrightarrow \neg D$$

Copyright © Albert R. Meyer, 2007. All rights reserved. February 9, 2007

lec 1F.26

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

Math vs. English

Mathematician:
"If a function is not continuous,
then it is not differentiable."

$$C \longrightarrow D \quad ? \text{ NO!}$$

Copyright © Albert R. Meyer, 2007. All rights reserved. February 9, 2007

lec 1F.27

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

Deductions

From: P implies Q , Q implies R

Conclude: P implies R

$$\frac{\overbrace{(P \rightarrow Q), (Q \rightarrow R)}^{\text{Antecedents}}}{\underbrace{P \rightarrow R}_{\text{Conclusion}}}$$

Copyright © Albert R. Meyer, 2007. All rights reserved. February 9, 2007

lec 1F.28

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

Sound Rules

Definition: A rule is *sound* if the
conclusion is true whenever **all**
antecedents are true.

Copyright © Albert R. Meyer, 2007. All rights reserved. February 9, 2007

lec 1F.29

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

A Sound Deduction

$$\frac{P \rightarrow Q, \quad P}{Q}$$

Modus ponens

Copyright © Albert R. Meyer, 2007. All rights reserved. February 9, 2007

lec 1F.30

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

A Sound Deduction

$$\frac{1 = -1}{\text{Russell is the Pope}}$$

Copyright © Albert R. Meyer, 2007. All rights reserved. February 9, 2007

lec 1F.31

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

An Unsound Deduction

$$\frac{\bar{P} \rightarrow \bar{Q}}{P \rightarrow Q}$$

Copyright © Albert R. Meyer, 2007. All rights reserved. February 9, 2007

lec 1F.32

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

An Unsound Deduction

$$\frac{\text{not Smart} \rightarrow \text{not MIT-student}}{\text{Smart} \rightarrow \text{MIT-student}} \quad \begin{array}{l} \text{Yes!} \\ \text{No!} \end{array}$$

Copyright © Albert R. Meyer, 2007. All rights reserved. February 9, 2007

lec 1F.33

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

Team Problem

Problems 2 & 3

Copyright © Albert R. Meyer, 2007. All rights reserved. February 9, 2007

lec 1F.34

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

Mathematics for Computer Science
MIT 6.042J/18.062J

Propositional Logic, II

Proof by Cases
Proof by Contradiction

Feb. 12, 2007

Copyright © Albert R. Meyer, 2007. All rights reserved.

lec 2M.1

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

Proof by Truth Tables

DeMorgan's Law

$\neg (P \vee Q)$ is equivalent to $\bar{P} \wedge \bar{Q}$

P	Q	$\neg (P \vee Q)$
T	T	F
T	F	F
F	T	F
F	F	T

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

Feb. 12, 2007

Copyright © Albert R. Meyer, 2007. All rights reserved.

lec 2M.2

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

Proof by Deductions

A student is trying to prove that propositions P , Q , and R are all true. She proceeds as follows.

First, she proves three facts:

- P implies Q
- Q implies R
- R implies P .

Then she concludes,

"Thus P , Q , and R are obviously all true."

Feb. 12, 2007

Copyright © Albert R. Meyer, 2007. All rights reserved.

lec 2M.3

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

Proposed Deduction Rule

From: P implies Q , Q implies R , R implies P

Conclude: P , Q , and R are true.

$$\frac{(P \rightarrow Q), (Q \rightarrow R), (R \rightarrow P)}{P \wedge Q \wedge R}$$

Feb. 12, 2007

Copyright © Albert R. Meyer, 2007. All rights reserved.

lec 2M.4

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

Sound Rule?

Conclusion true whenever all antecedents true.

$$P \rightarrow Q \quad Q \rightarrow R \quad R \rightarrow P \quad P \wedge Q \wedge R$$

Antecedents

Conclusion

Feb. 12, 2007

Copyright © Albert R. Meyer, 2007. All rights reserved.

lec 2M.5

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

Sound Rule?

Conclusion true whenever all antecedents true.

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

$$P \rightarrow Q \quad Q \rightarrow R \quad R \rightarrow P \quad P \wedge Q \wedge R$$

Antecedents

Conclusion

Feb. 12, 2007

Copyright © Albert R. Meyer, 2007. All rights reserved.

lec 2M.6

6

9

13

7

12

10

5

3

1

4

14

15

8

11

2

Sound Rule?

Conclusion true whenever all antecedents true.

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

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

P ∧ Q ∧ R	sound?
T	
F	
F	
F	
F	
F	
F	
F	
F	

Antecedents

Conclusion

Feb. 12, 2007Copyright © Albert R. Meyer, 2007. All rights reserved.lec 2M.7

6

9

13

7

12

10

5

3

1

4

14

15

8

11

2

Sound Rule?

Conclusion true whenever all antecedents true.

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

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

P ∧ Q ∧ R	sound?
T	
F	OK
F	OK
F	OK
F	OK
F	OK
F	OK
F	OK
F	

Feb. 12, 2007Copyright © Albert R. Meyer, 2007. All rights reserved.lec 2M.8

6

9

13

7

12

10

5

3

1

4

14

15

8

11

2

Sound Rule?

Conclusion true whenever all antecedents true.

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

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

P ∧ Q ∧ R	sound?
T	OK
F	OK
F	OK
F	OK
F	OK
F	OK
F	OK
F	OK
F	

Feb. 12, 2007Copyright © Albert R. Meyer, 2007. All rights reserved.lec 2M.9

6

9

13

7

12

10

5

3

1

4

14

15

8

11

2

Sound Rule?

Conclusion true whenever all antecedents true.

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

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

P ∧ Q ∧ R	sound?
T	OK
F	OK
F	OK
F	OK
F	OK
F	OK
F	OK
F	OK
F	

Feb. 12, 2007Copyright © Albert R. Meyer, 2007. All rights reserved.lec 2M.10

6

9

13

7

12

10

5

3

1

4

14

15

8

11

2

Sound Rule?

Conclusion true whenever all antecedents true.

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

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

P ∧ Q ∧ R	sound?
T	OK
F	OK
F	OK
F	OK
F	OK
F	OK
F	OK
F	OK
F	NOT OK!

Feb. 12, 2007Copyright © Albert R. Meyer, 2007. All rights reserved.lec 2M.11

6

9

13

7

12

10

5

3

1

4

14

15

8

11

2

Reasoning by Cases

Quicker proof of unsoundness than from truth tables

Feb. 12, 2007Copyright © Albert R. Meyer, 2007. All rights reserved.lec 2M.12

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

Quicker by Cases

$$\frac{P \rightarrow Q, Q \rightarrow R, R \rightarrow P}{P \wedge Q \wedge R}$$

Case 1: P is **true**. Now, if antecedents are true, then Q must be true (because P implies Q). Then R must be true (because Q implies R). So the conclusion $P \wedge Q \wedge R$ is true.
This case is **OK**.

Feb. 12, 2007

Copyright © Albert R. Meyer, 2007. All rights reserved.

lec 2M.13

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

Quicker by Cases

$$\frac{P \rightarrow Q, Q \rightarrow R, R \rightarrow P}{P \wedge Q \wedge R}$$

Case 2: P is **false**. To make antecedents **true**, R must be **false** (because R implies P), so Q must be **false** (because Q implies R). This assignment does make the antecedents **true**, but the conclusion $P \wedge Q \wedge R$ is (very) **false**.
This case is **not OK**.

Feb. 12, 2007

Copyright © Albert R. Meyer, 2007. All rights reserved.

lec 2M.14

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

Goldbach Conjecture

Every even integer greater than 2 is the sum of two primes.

Evidence: $4 = 2 + 2$
 $6 = 3 + 3$
 $8 = 5 + 3$
 \vdots
 $20 = ? \quad 13 + 7$

Feb. 12, 2007

Copyright © Albert R. Meyer, 2007. All rights reserved.

lec 2M.15

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

Goldbach Conjecture

True for all even numbers with up to **13 digits!**

(Rosen, p.182)

It remains an **OPEN problem**:
no counterexample, no proof.
UNTIL NOW!...

Feb. 12, 2007

Copyright © Albert R. Meyer, 2007. All rights reserved.

lec 2M.16

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

Goldbach Conjecture

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

Feb. 12, 2007

Copyright © Albert R. Meyer, 2007. All rights reserved.

lec 2M.17

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

Team Problem

Problem 1

Feb. 12, 2007

Copyright © Albert R. Meyer, 2007. All rights reserved.

lec 2M.18

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

Proof by Contradiction

$$\frac{\bar{P} \rightarrow \mathbf{F}}{P}$$

Feb. 12, 2007

Copyright © Albert R. Meyer, 2007. All rights reserved.

lec 2M.19

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

Proof by Contradiction

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

Proof (by contradiction):

- Suppose $\sqrt{2}$ was rational.
- Choose m, n integers without common prime factors (always possible) such that

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

- Show that m & n are both even, a contradiction!

Feb. 12, 2007

Copyright © Albert R. Meyer, 2007. All rights reserved.

lec 2M.20

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

Proof by Contradiction

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

Proof (by contradiction):

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

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

$$2n^2 = m^2$$

so m is even.

so can assume $m = 2l$

$$m^2 = 4l^2$$

$$2n^2 = 4l^2$$

$$n^2 = 2l^2$$

so n is even.

Feb. 12, 2007

Copyright © Albert R. Meyer, 2007. All rights reserved.

lec 2M.21

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

Quickie

Proof assumes that

If m^2 is even, then m is even.

Why!

Feb. 12, 2007

Copyright © Albert R. Meyer, 2007. All rights reserved.

lec 2M.22

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

Team Problem

Problems 2 & 3

Feb. 12, 2007

Copyright © Albert R. Meyer, 2007. All rights reserved.

lec 2M.23



Predicate Logic

Quantifiers \forall, \exists



Predicates

Predicates are
Propositions with variables

Example:

$$P(x,y) \stackrel{\text{::=}}{=} x + 2 = y$$

“is defined to be”



Predicates

$$P(x, y) ::= [x + 2 = y]$$

$x = 1$ and $y = 3$: $P(1,3)$ is true

$x = 1$ and $y = 4$: $P(1,4)$ is false
 $\neg P(1,4)$ is true



Quantifiers

$\forall x$ For ALL x

$\exists y$ There EXISTS some y



Quantifiers

x, y range over **Domain of Discourse**

$$\forall x \exists y. x < y$$

<u>Domain</u>	<u>Truth value</u>
integers \mathbb{Z}	True
positive integers \mathbb{Z}^+	True
negative integers \mathbb{Z}^-	False
negative reals \mathbb{R}^-	True



$\forall \alpha$ versus $\exists d$

~~$\forall \alpha \in \text{attack}$~~ ~~$\exists d \in \text{defense}$~~ .
 d protects against α

For every attack, I have a defense:
against MYDOOM, use Defender
against ILOVEYOU, use Norton
against BABLAS, use Zonealarm ...

$\forall \exists$ is expensive!

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

$\exists \forall$

$\exists d \in \text{defense } \forall a \in \text{attack.}$
d protects against *a*

I have *one* defense good
 against every attack.

Example: *d* is MITviruscan,
 protects against *all* viruses

Copyright © Albert R. Meyer, 2007. All rights reserved. February 14, 2007

lec 2W.8

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

So $\exists \forall$ is better here

$\exists d \in \text{defense } \forall a \in \text{attack.}$
d protects against *a*

I have *one* defense good
 against every attack.

That's what we want!

Copyright © Albert R. Meyer, 2007. All rights reserved. February 14, 2007

lec 2W.9

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

Math vs. English

Poet:

“All that $\overbrace{\text{glitters}}^G$ is not $\overbrace{\text{gold}}^{Au}$.”

$\forall x. G(x) \rightarrow \neg Au(x)$

No!: gold glitters like gold

Copyright © Albert R. Meyer, 2007. All rights reserved. February 14, 2007

lec 2W.10

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

Math vs. English

Poet:

“All that glitters is not gold.” *necessarily*

$\neg [\forall x. G(x) \rightarrow \neg Au(x)]$

(Poetic license)

Copyright © Albert R. Meyer, 2007. All rights reserved. February 14, 2007

lec 2W.11

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

Math vs. English

Poet: “There is a season for every
 purpose under heaven”

$\exists s \in \text{Season } \forall p \in \text{Purpose. } s \text{ is for } p$

So some season, say Spring, is good for
 all Purposes?

NO, Spring is no good for snow shoveling

Copyright © Albert R. Meyer, 2007. All rights reserved. February 14, 2007

lec 2W.12

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

Poetic license again:

Poet: “There is a season for every
 purpose under heaven”

$\exists s \in \text{Season } \forall p \in \text{Purpose. } s \text{ is for } p$

Poet's meaning flips the quantifiers

Copyright © Albert R. Meyer, 2007. All rights reserved. February 14, 2007

lec 2W.13

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

Poetic license again:

Poet: “There is a season for every purpose under heaven”

$\forall p \in \text{Purpose} \exists s \in \text{Season}. s$ is for p
 for snow shoveling, *Winter* is good
 for planting, *Spring* is good
 for leaf watching, *Fall* is good
 etc.

Copyright © Albert R. Meyer, 2007. All rights reserved. February 14, 2007

lec 2W.14

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

Team Problems

Problems 1 & 2

Copyright © Albert R. Meyer, 2007. All rights reserved. February 14, 2007

lec 2W.15

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

Propositional Validity

$$(A \rightarrow B) \vee (B \rightarrow A)$$

True *no matter what* the truth values of A and B are

Copyright © Albert R. Meyer, 2007. All rights reserved. February 14, 2007

lec 2W.16

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

Predicate Calculus Validity

$$\forall z [Q(z) \wedge P(z)] \rightarrow [\forall x.Q(x) \wedge \forall y.P(y)]$$

True *no matter what*

- the Domain is,
- or the predicates are.

Copyright © Albert R. Meyer, 2007. All rights reserved. February 14, 2007

lec 2W.17

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

Not Valid

$$\forall z [Q(z) \vee P(z)] \rightarrow [\forall x.Q(x) \vee \forall y.P(y)]$$

Proof: Give *countermodel*, where $\forall z [Q(z) \vee P(z)]$ is **true**,
 but $\forall x.Q(x) \vee \forall y.P(y)$ is **false**.

Namely, let domain $::= \{e, \pi\}$,
 $Q(z) ::= [z = e]$,
 $P(z) ::= [z = \pi]$.

Copyright © Albert R. Meyer, 2007. All rights reserved. February 14, 2007

lec 2W.18

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

Predicate Calculus Validity

$$\forall z [Q(z) \wedge P(z)] \rightarrow [\forall x.Q(x) \wedge \forall y.P(y)]$$

Proof strategy: We assume

$$\forall z [Q(z) \wedge P(z)]$$

to prove

$$\forall x.Q(x) \wedge \forall y.P(y)$$

Copyright © Albert R. Meyer, 2007. All rights reserved. February 14, 2007

lec 2W.19

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

Universal Generalization (UG)

$$\frac{A \rightarrow R(c)}{A \rightarrow \forall x.R(x)}$$

providing c does not occur in A

Copyright © Albert R. Meyer, 2007. All rights reserved. February 14, 2007

lec 2W.20

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

Validities

$$\forall z [Q(z) \wedge P(z)] \rightarrow [\forall x.Q(x) \wedge \forall y.P(y)]$$

Proof: Assume $\forall z [Q(z) \wedge P(z)]$.

So $Q(z) \wedge P(z)$ holds for all z in the domain.

Now let c be some domain element. So

$Q(c) \wedge P(c)$ holds, and therefore $Q(c)$ by itself holds.

But c could have been any element of the domain.

So we conclude $\forall x.Q(x)$. (by **UG**)

We conclude $\forall y.P(y)$ similarly. Therefore,

$$\forall x.Q(x) \wedge \forall y.P(y) \quad \text{QED.}$$

Copyright © Albert R. Meyer, 2007. All rights reserved. February 14, 2007

lec 2W.21

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

More Validities

$$\forall x[P(x) \vee A] \leftrightarrow [\forall x.P(x)] \vee A$$

providing x does not occur in A

$$[\neg \forall x.P(x)] \leftrightarrow [\exists x.\neg P(x)]$$

(version of DeMorgan)

Copyright © Albert R. Meyer, 2007. All rights reserved. February 14, 2007

lec 2W.22

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

Team Problems

Problems

4 & 3

Copyright © Albert R. Meyer, 2007. All rights reserved. February 14, 2007

lec 2W.23

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

Sets & Functions

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

What is a Set?

Informally:

A *set* is a collection of mathematical objects, with the collection treated as a single mathematical object.

(This is *circular* of course:
what's a collection?)

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

Some sets

real numbers, \mathbb{R}
complex numbers, \mathbb{C}
integers, \mathbb{Z}
empty set, \emptyset
set of all subsets of integers, $\text{pow}(\mathbb{Z})$
the *power* set

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

Some sets

$\{7, \text{"Albert R."}, \pi/2, \mathbf{T}\}$

A set with 4 *elements*: two numbers, a string, and a Boolean value.

Same as

$\{\text{"Albert R."}, 7, \mathbf{T}, \pi/2\}$

-- order doesn't matter

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

Membership

$x \in A$ x is an *element* of A

$\pi/2 \in \{7, \text{"Albert R."}, \pi/2, \mathbf{T}\}$

$\pi/3 \notin \{7, \text{"Albert R."}, \pi/2, \mathbf{T}\}$

$14/2 \in \{7, \text{"Albert R."}, \pi/2, \mathbf{T}\}$

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

Synonyms for Membership

$x \in A$ x is a *member* of A

x is *in* A

Examples:

$7 \in \mathbb{Z}$ $2/3 \notin \mathbb{Z}$ $\mathbb{Z} \in \text{pow}(\mathbb{R})$

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

In or Not In

An element is **in** or **not in** a set:

$\{7, \pi/2, 7\}$ is same as $\{7, \pi/2\}$

(No notion of being in the set more than once)

Copyright © Albert R. Meyer, 2007. All rights reserved. February 16, 2007

lec 2F.7

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

Containment

$A \subseteq B$ A is a **subset** of B
 A is **contained in** B

Every element of A is also an element of B .

$\mathbb{Z} \subseteq \mathbb{R}$, $\mathbb{R} \subseteq \mathbb{C}$, $\{3\} \subseteq \{5, 7, 3\}$

$\emptyset \subseteq$ every set, $A \subseteq A$

Copyright © Albert R. Meyer, 2007. All rights reserved. February 16, 2007

lec 2F.8

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

Defining Sets

The **set of elements**, x , in A
such that $P(x)$ is true.

$\{x \in A \mid P(x)\}$

Copyright © Albert R. Meyer, 2007. All rights reserved. February 16, 2007

lec 2F.9

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

Defining Sets

The set of **even** integers:
 $\{n \in \mathbb{Z} \mid n \text{ is even}\}$

Copyright © Albert R. Meyer, 2007. All rights reserved. February 16, 2007

lec 2F.10

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

New sets from old

union:

$A \cup B ::= \{x \mid (x \in A) \vee (x \in B)\}$

intersection:

$A \cap B ::= \{x \mid x \in A \wedge x \in B\}$

difference:

$A - B ::= \{x \mid (x \in A) \wedge (x \notin B)\}$

Copyright © Albert R. Meyer, 2007. All rights reserved. February 16, 2007

lec 2F.11

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

power set

$\text{pow}(A) ::= \{S \mid S \subseteq A\}$

$\text{pow}(\{a, b\}) = \{\{a, b\}, \{a\}, \{b\}, \emptyset\}$

Copyright © Albert R. Meyer, 2007. All rights reserved. February 16, 2007

lec 2F.17

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

Quickie

What is $\text{Pow}(\emptyset)$?

Ans: $\{\emptyset\}$

What is $\text{Pow}(\text{Pow}(\emptyset))$?

Ans: $\{\{\emptyset\}, \emptyset\}$

Copyright © Albert R. Meyer, 2007. All rights reserved. February 16, 2007

lec 2F.18

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

Russell's Paradox

Let $W := \{S \in \text{Sets} \mid S \notin S\}$

so $S \in W \leftrightarrow S \notin S$

Let S be W and reach a contradiction:

$W \in W \leftrightarrow W \notin W$

Copyright © Albert R. Meyer, 2007. All rights reserved. February 16, 2007

lec 2F.19

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

Russell's Paradox

The fallacy: **W is not a set!**

No set is a member of itself, so
 W = the collection of all sets,
 which is **not** a set!

Copyright © Albert R. Meyer, 2007. All rights reserved. February 16, 2007

lec 2F.20

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

Team Problems

Problems

1 & 3

Copyright © Albert R. Meyer, 2007. All rights reserved. February 16, 2007

lec 2F.21

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

Mathematics for Computer Science

MIT 6.042J/18.062J

Functions

Copyright © Albert R. Meyer, 2007. All rights reserved. February 16, 2007

lec 2F.25

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

$f : A \rightarrow B$

function, f , from set A to set B

associates an element, $f(a) \in B$
 with an element $a \in A$.

Example: f is the string-length
 function: $f(\text{"aabd"}) = 4$

Copyright © Albert R. Meyer, 2007. All rights reserved. February 16, 2007

lec 2F.26

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

$$f: \text{Strings} \rightarrow \mathbb{N}$$

The *domain* of f is the set of strings.

The *codomain* of f is the set of nonnegative integers

Copyright © Albert R. Meyer, 2007. All rights reserved. February 16, 2007

lec 2F.27

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

$$g(x, y) ::= \frac{1}{x - y}$$

$$g: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$$

domain(g) = all pairs of reals

codomain(g) = all reals

But g is *partial*:

not defined on pairs (r, r)

Copyright © Albert R. Meyer, 2007. All rights reserved. February 16, 2007

lec 2F.28

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

Total functions

$f: A \rightarrow B$ is *total* iff every element of A is assigned a B -value by f

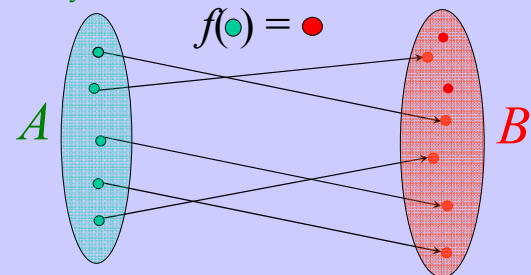
Copyright © Albert R. Meyer, 2007. All rights reserved. February 16, 2007

lec 2F.30

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

Total functions

exactly 1 arrow out



Copyright © Albert R. Meyer, 2007. All rights reserved. February 16, 2007

lec 2F.31

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

Surjections

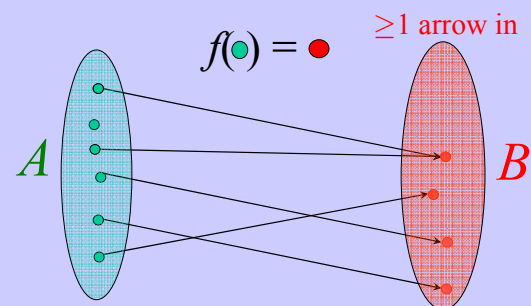
$f: A \rightarrow B$ is a *surjection* iff every element of B is f of something

Copyright © Albert R. Meyer, 2007. All rights reserved. February 16, 2007

lec 2F.33

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

Surjection



Copyright © Albert R. Meyer, 2007. All rights reserved. February 16, 2007

lec 2F.34

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

Mapping Rule

surjection $A \rightarrow B$ implies
 $|A| \geq |B|$

Copyright © Albert R. Meyer, 2007. All rights reserved. February 16, 2007

lec 2F.36

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

Injections

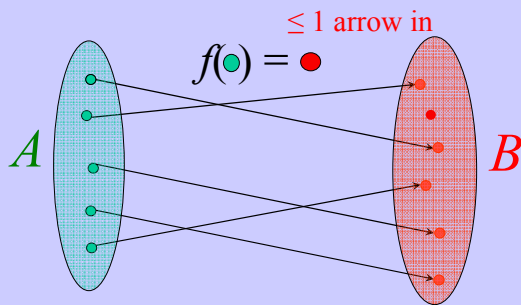
$f : A \rightarrow B$ is an *injection*
 iff every element of B is
 f of *at most* 1 thing

Copyright © Albert R. Meyer, 2007. All rights reserved. February 16, 2007

lec 2F.37

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

Injections



Copyright © Albert R. Meyer, 2007. All rights reserved. February 16, 2007

lec 2F.38

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

Mapping Rule

injection $A \rightarrow B$ implies
 $|A| \leq |B|$
total

Copyright © Albert R. Meyer, 2007. All rights reserved. February 16, 2007

lec 2F.40

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

Bijections

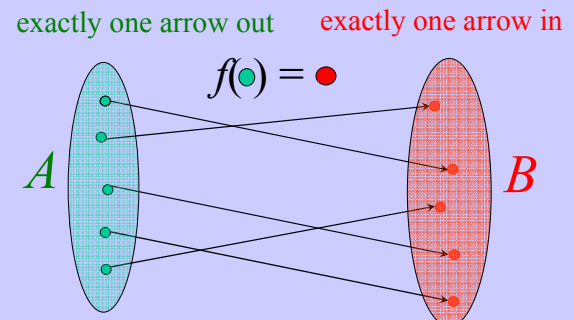
$f : A \rightarrow B$ is a *bijection* iff
 it is all those good things:
 total, onto, and 1-1

Copyright © Albert R. Meyer, 2007. All rights reserved. February 16, 2007

lec 2F.42

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

Bijections



Copyright © Albert R. Meyer, 2007. All rights reserved. February 16, 2007

lec 2F.43

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

Mapping Rule

bijection $A \rightarrow B$ implies
 $|A| = |B|$

Copyright © Albert R. Meyer, 2007. All rights reserved. February 16, 2007

lec 2F.44

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

Team Problems

Problem 2

Copyright © Albert R. Meyer, 2007. All rights reserved. February 16, 2007

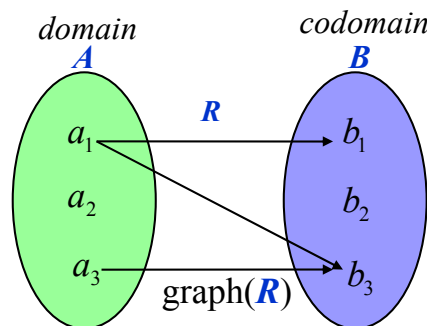
lec 2F.46

4	9	13	7
12	10	16	5
3	1	6	14
15	8	11	2

Partial Orders & Scheduling

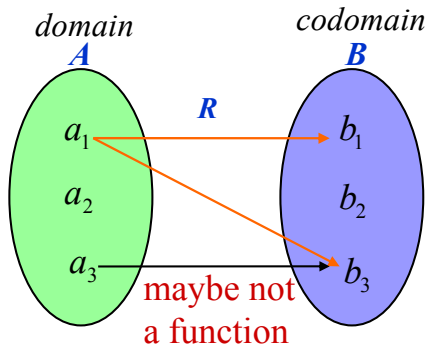
4	9	13	7
12	10	16	5
3	1	6	14
15	8	11	2

Binary relation R from A to B



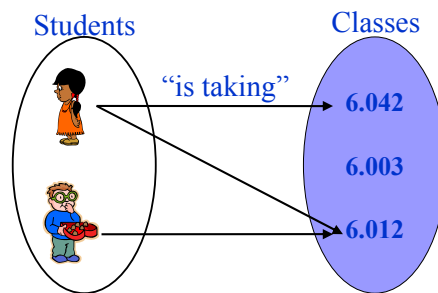
4	9	13	7
12	10	16	5
3	1	6	14
15	8	11	2

Binary relation R from A to B



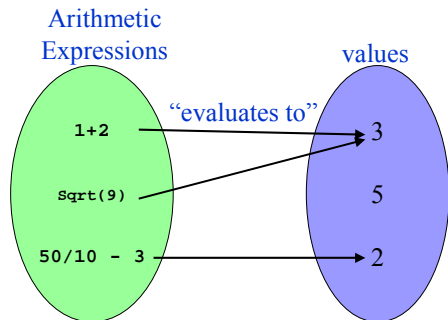
4	9	13	7
12	10	16	5
3	1	6	14
15	8	11	2

Example



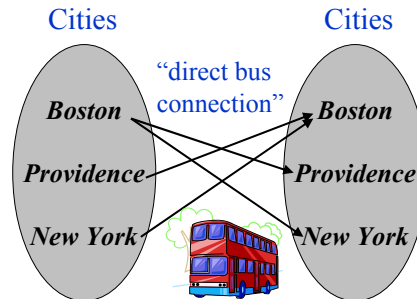
4	9	13	7
12	10	16	5
3	1	6	14
15	8	11	2

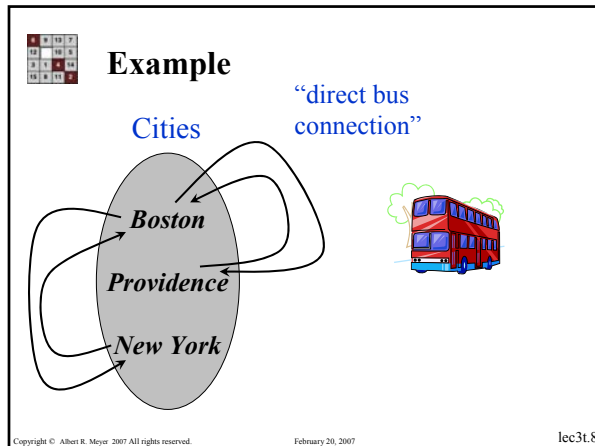
Example




4	9	13	7
12	10	16	5
3	1	6	14
15	8	11	2

Example







 **Some Course 6 Prerequisites**

18.01 \rightarrow 6.042	18.03, 8.02 \rightarrow 6.002
18.01 \rightarrow 18.02	6.001, 6.002 \rightarrow 6.004
18.01 \rightarrow 18.03	6.001, 6.002 \rightarrow 6.003
8.01 \rightarrow 8.02	6.004 \rightarrow 6.033
6.001 \rightarrow 6.034	6.033 \rightarrow 6.857
6.042 \rightarrow 6.046	6.046 \rightarrow 6.840


Copyright © Albert R. Meyer, 2007. All rights reserved. February 20, 2007 lec3t.9

 **Subject Prerequisites** 

subject c is a direct prerequisite for subject d


$$c \rightarrow d$$

Copyright © Albert R. Meyer, 2007. All rights reserved. February 20, 2007 lec3t.10

 **Direct Prerequisites**

$$18.01 \rightarrow 6.042 \rightarrow 6.046 \rightarrow 6.840$$


Copyright © Albert R. Meyer, 2007. All rights reserved. February 20, 2007 lec3t.11

 **Indirect Prerequisites**

$$18.01 \rightarrow 6.042 \rightarrow 6.046 \rightarrow 6.840$$

18.01 is *indirect prereq.* of 6.840
(\rightarrow is *transitive closure* of \rightarrow)

Copyright © Albert R. Meyer, 2007. All rights reserved. February 20, 2007 lec3t.12

 **"Freshman subjects"**

18.01 **8.01** **6.001**

subjects with no prereqs:

d is a Freshman subject iff

$$\langle \text{nothing} \rangle \rightarrow d$$

d is *minimal*

Copyright © Albert R. Meyer, 2007. All rights reserved. February 20, 2007 lec3t.13



minimal not minimum

minimum means "smallest"
-- a prereq. for *every* subject
no minimum in this example

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 20, 2007

lec3t.15



Constructing a Term Schedule

- 18.01 → 6.042
- 18.01 → 18.02
- 18.01 → 18.03
- 8.01 → 8.02
- 6.001 → 6.034
- 6.042 → 6.046
- 18.03, 8.02 → 6.002
- 6.001, 6.002 → 6.004
- 6.001, 6.002 → 6.003
- 6.004 → 6.033
- 6.033 → 6.857
- 6.046 → 6.840

identify *minimal* elements

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 20, 2007

lec3t.16



Constructing a Term Schedule

18.01

8.01

6.001

start schedule with them

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 20, 2007

lec3t.17



Constructing a Term Schedule

- ~~18.01~~ → 6.042
- 18.01 → 18.02
- 18.01 → 18.03
- ~~8.01~~ → 8.02
- ~~6.001~~ → 6.034
- 6.042 → 6.046
- 18.03, 8.02 → 6.002
- ~~6.001~~, 6.002 → 6.004
- ~~6.001~~, 6.002 → 6.003
- 6.004 → 6.033
- 6.033 → 6.857
- 6.046 → 6.840

remove minimal elements

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 20, 2007

lec3t.18



Constructing a Term Schedule

- 6.042
- 18.02
- 18.03
- 8.02
- 6.034
- 6.042 → 6.046
- 18.03, 8.02 → 6.002
- 6.002 → 6.004
- 6.002 → 6.003
- 6.004 → 6.033
- 6.033 → 6.857
- 6.046 → 6.840

identify new minimal elements

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 20, 2007

lec3t.20



Constructing a Term Schedule



schedule them next

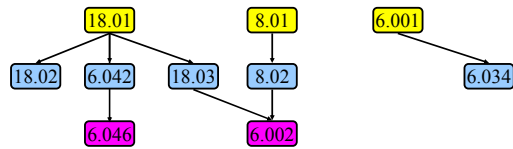
Copyright © Albert R. Meyer, 2007. All rights reserved.

February 20, 2007

lec3t.21

4	9	13	7
12	10	6	5
3	1	8	14
15	11	16	2

Constructing a Term Schedule



continue in this way...

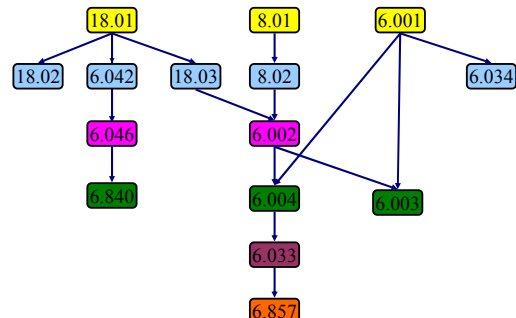
Copyright © Albert R. Meyer, 2007. All rights reserved.

February 20, 2007

lec3t.22

4	9	13	7
12	10	6	5
3	1	8	14
15	11	16	2

Complete Term Schedule



Copyright © Albert R. Meyer, 2007. All rights reserved.

February 20, 2007

lec3t.23

4	9	13	7
12	10	6	5
3	1	8	14
15	11	16	2

Antichains

Set of subjects with no prereqs among them

-- can be taken in *any order*.
(said to be *incomparable*)

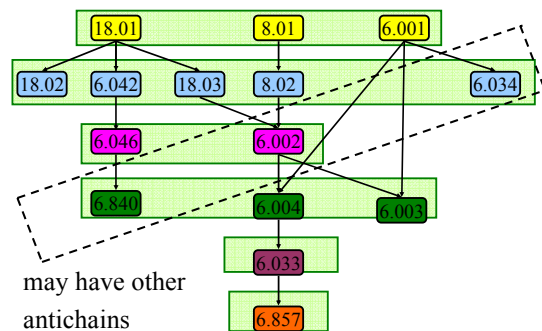
Copyright © Albert R. Meyer, 2007. All rights reserved.

February 20, 2007

lec3t.24

4	9	13	7
12	10	6	5
3	1	8	14
15	11	16	2

Some Antichains



Copyright © Albert R. Meyer, 2007. All rights reserved.

February 20, 2007

lec3t.25

4	9	13	7
12	10	6	5
3	1	8	14
15	11	16	2

Chains

Set of successive prereqs

-- must be taken in order.
(subjects said to be *comparable*)

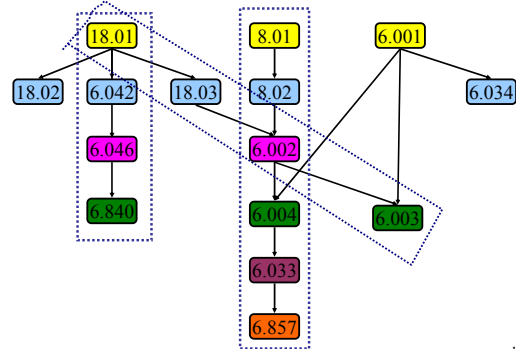
Copyright © Albert R. Meyer, 2007. All rights reserved.

February 20, 2007

lec3t.26

4	9	13	7
12	10	6	5
3	1	8	14
15	11	16	2

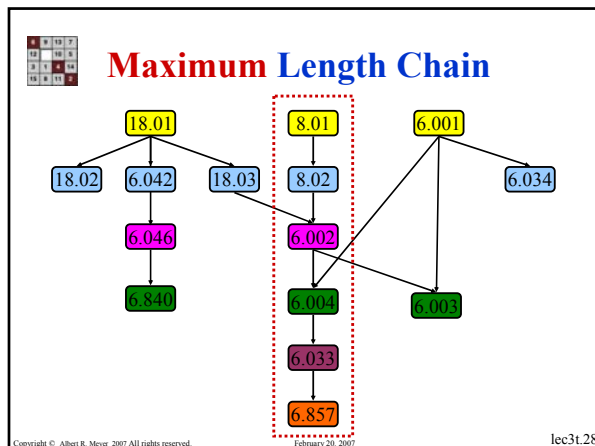
Some Chains



Copyright © Albert R. Meyer, 2007. All rights reserved.

February 20, 2007

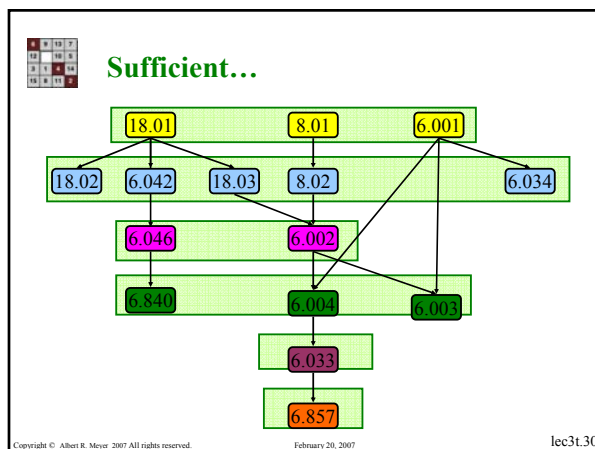
lec3t.27



How many terms to graduate?

- 6 terms are **necessary** to complete the curriculum
- *and* **sufficient** (if you can take unlimited subjects per term...)

Copyright © Albert R. Meyer, 2007. All rights reserved. February 20, 2007 lec3t.29

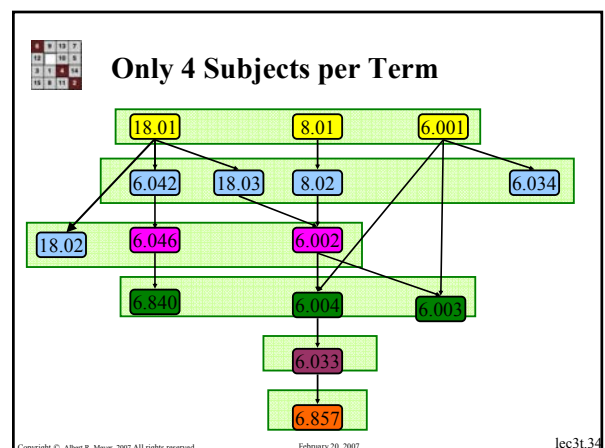
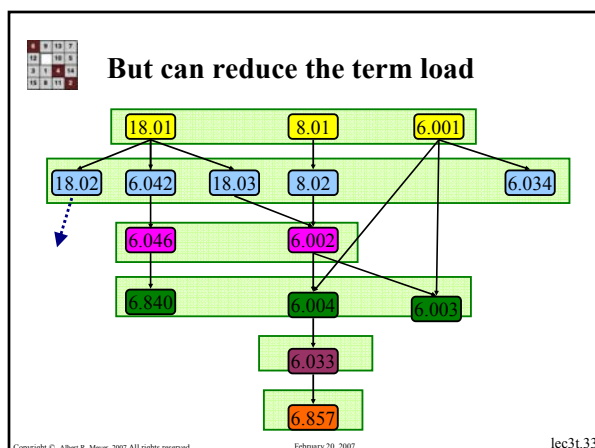


Parallel Processing Time

min parallel time = max chain size
 required # processors
 (term load in this case)

\leq max antichain size
 5 in this case

Copyright © Albert R. Meyer, 2007. All rights reserved. February 20, 2007 lec3t.31



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

3 Subjects per Term Possible



Copyright © Albert R. Meyer, 2007. All rights reserved.

February 20, 2007

lec3t.36

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

A 3-course term is **necessary**

- 15 subjects
 - max chain size = 6
 - size of *some* block must be $\geq \lceil 15/6 \rceil = 3$.
- \therefore to finish in 6 terms, must take ≥ 3 subjects some term

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 20, 2007

lec3t.38

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

Parallel Task Scheduling

Theorem: If the longest chain has size t , then the subjects can be *partitioned* into t successive antichains, with all prerequisites of an antichain in earlier ones.

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 20, 2007

lec3t.39

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

Dilworth's Lemma

Prereq's among n subjects has

- a chain of size $\geq t$, *or*
- or an antichain of size $\geq \left\lceil \frac{n}{t} \right\rceil$

for all $1 \leq t \leq n$.

Copyright © Albert R. Meyer, 2007. All rights reserved.

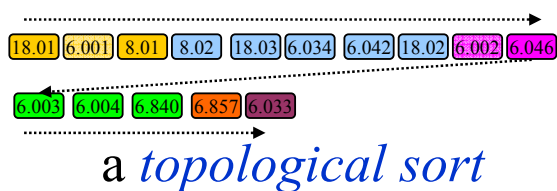
February 20, 2007

lec3t.40

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

A Leisurely Schedule

Graduate taking only 1 subject/term?
Sure,



Copyright © Albert R. Meyer, 2007. All rights reserved.

February 20, 2007

lec3t.44

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

Team Problem

Problem 1

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 20, 2007

lec3t.45

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

Partial Orders

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 20, 2007

lec3t.46

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

Subject Prerequisites

If subjects c, d are *mutual prereq's*:

$$c \rightarrow d, \text{ and } d \rightarrow c$$

then no one can graduate!

Comm. on Curricula ensures:

$$\text{if } c \rightarrow d, \text{ then } \neg (d \rightarrow c)$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 20, 2007

lec3t.47

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

Asymmetry

Binary relation, R , on set A ,
is *asymmetric* iff

$$aRb \text{ implies } \neg(bRa)$$

for all $a, b \in A$

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 20, 2007

lec3t.48

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

Transitivity

Binary relation, R , on set A ,
is *transitive*:

$$aRb \text{ and } bRc \text{ implies } aRc$$

for all $a, b, c \in A$.

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 20, 2007

lec3t.49

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

Strict Partial Orders

Binary relation, R , on set A ,
is a *strict partial order* iff

- it is *transitive* and
- *asymmetric*

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 20, 2007

lec3t.50

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

Some Partial Orders

- \leq on the Integers
 - $<$ on the Reals
 - \subseteq on Sets (subset)
 - \subset on Sets (*proper* subset)
- } total

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 20, 2007

lec3t.53

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

Total Order on A

Partial Order, R , such that

$$aRb \text{ or } bRa$$

for all $a \neq b \in A$

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 20, 2007

lec3t.54

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

Partial Orders

• $y \ll x$ (*much less than*)
(say, $y + 2 \leq x$)

¬ $[3 \ll 4]$ and ¬ $[4 \ll 3]$

incomparable

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 20, 2007

lec3t.55

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

Representing Partial Orders

The subset relation,

\subseteq

on sets is the *canonical*
example of weak partial order

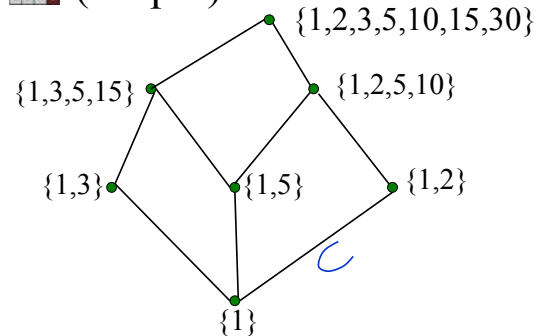
Copyright © Albert R. Meyer, 2007. All rights reserved.

February 20, 2007

lec3t.56

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

(Proper) Subset Relation



Copyright © Albert R. Meyer, 2007. All rights reserved.

February 20, 2007

lec3t.57

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

Partial Order: *divides*

a *divides* b iff
 $ka = b$ for some $k \in \mathbb{N}$

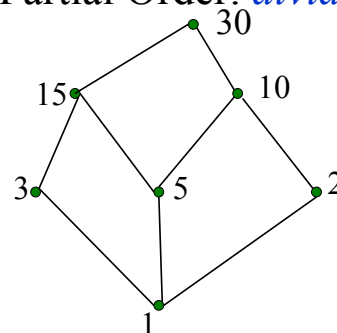
Copyright © Albert R. Meyer, 2007. All rights reserved.

February 20, 2007

lec3t.58

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

Partial Order: *divides*



Copyright © Albert R. Meyer, 2007. All rights reserved.

February 20, 2007

lec3t.59

4	9	13	7
12	10	16	5
3	1	6	14
15	8	11	2

Divides & Subset

same "shape"

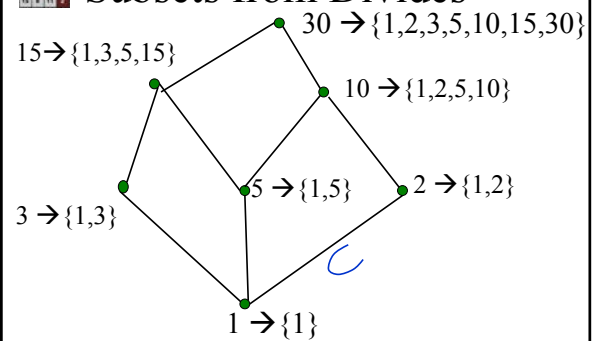
Copyright © Albert R. Meyer, 2007. All rights reserved.

February 20, 2007

lec3t.60

4	9	13	7
12	10	16	5
3	1	6	14
15	8	11	2

Subsets from Divides



Copyright © Albert R. Meyer, 2007. All rights reserved.

February 20, 2007

lec3t.61

4	9	13	7
12	10	16	5
3	1	6	14
15	8	11	2

Team Problems

Problems 2–4

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 20, 2007

lec3t.66

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

Induction

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 21, 2007

lec 3w.1

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

Example of Induction

Suppose we have a property (say *color*) of the nonnegative integers:

0, 1, 2, 3, 4, 5, ...

If 0 is *red*, and a number *next to* a red number is *red*, then *all numbers are red*!

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 21, 2007

lec 3w.2

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

The Induction Rule

0 and (from *n* to *n+1*),
proves 0, 1, 2, 3,

$$\frac{R(0), \quad \forall n \in \mathbb{N}. R(n) \rightarrow R(n+1)}{\forall m \in \mathbb{N}. R(m)}$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 21, 2007

lec 3w.3

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

Like Dominos...



Copyright © Albert R. Meyer, 2007. All rights reserved.

February 21, 2007

lec 3w.4

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

Example Induction Proof

Let's prove:

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

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 21, 2007

lec 3w.5

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

Proof by Induction

Statements in *green* form a template for inductive proofs.

- Proof: (by induction on *n*)
- The induction hypothesis, *P(n)*, is:

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

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 21, 2007

lec 3w.6

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

Example Induction Proof

Base Case ($n = 0$):

$$\underbrace{1 + r + r^2 + \dots + r^0}_1 = \frac{r^{0+1} - 1}{r - 1} = \frac{r - 1}{r - 1} = 1$$

Wait: divide by zero bug!
This is only true for $r \neq 1$

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 21, 2007

lec 3w.7

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

Correction

Theorem:

$$\forall r \neq 1. \quad 1 + r + r^2 + \dots + r^n = \frac{r^{n+1} - 1}{r - 1}$$

Induction Hypothesis:

$$P(n) ::= \forall r \neq 1. \quad 1 + r + r^2 + \dots + r^n = \frac{r^{n+1} - 1}{r - 1}$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 21, 2007

lec 3w.8

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

An Example Proof

- Induction Step: Assume $P(n)$ for some $n \geq 0$ and prove $P(n+1)$:

$$\forall r \neq 1. \quad 1 + r + r^2 + \dots + r^{n+1} = \frac{r^{(n+1)+1} - 1}{r - 1}$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 21, 2007

lec 3w.9

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

An Example Proof

Have $P(n)$ by assumption:

$$\forall r \neq 1. \quad 1 + r + r^2 + \dots + r^n = \frac{r^{n+1} - 1}{r - 1}$$

So let $r \in \mathbb{C}$ be any number $\neq 1$.

Then from $P(n)$ we have

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

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 21, 2007

lec 3w.10

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

An Example Proof

adding r^{n+1} to both sides,

$$\begin{aligned} 1 + \dots + r^n + r^{n+1} &= \frac{r^{n+1} - 1}{r - 1} + r^{n+1} \\ &= \frac{r^{n+1} - 1 + r^{n+1}(r - 1)}{r - 1} \\ &= \frac{r^{(n+1)+1} - 1}{r - 1} \end{aligned}$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 21, 2007

lec 3w.11

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

An Example Proof

That is,

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

But since $r \neq 1$ was arbitrary, we conclude (by UG), that

$$\forall r \neq 1. \quad 1 + r + r^2 + \dots + r^{n+1} = \frac{r^{(n+1)+1} - 1}{r - 1}$$

which is $P(n+1)$.

• This completes the induction proof.
QED.

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 21, 2007

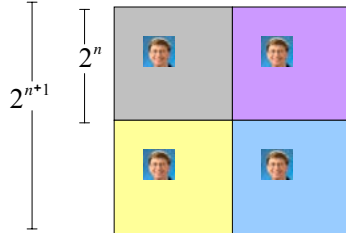
lec 3w.12

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

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

The Gehry/Gates Plaza

Induction step: assume can tile $2^n \times 2^n$,
prove can handle $2^{n+1} \times 2^{n+1}$.



Copyright © Albert R. Meyer, 2007. All rights reserved.

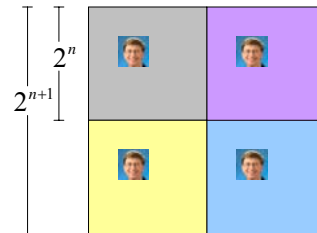
February 21, 2007

lec 3w.19

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

The Gehry/Gates Plaza

Now what?



Copyright © Albert R. Meyer, 2007. All rights reserved.

February 21, 2007

lec 3w.20

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

The Gehry/Gates Plaza

The fix:

Prove that we can always find
a tiling with Bill in the corner.

Copyright © Albert R. Meyer, 2007. All rights reserved.

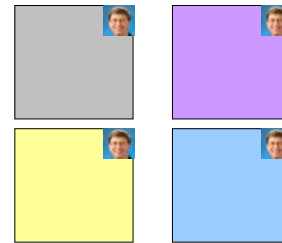
February 21, 2007

lec 3w.21

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

The Gehry/Gates Plaza

Note: Once have Bill in corner,
can get Bill in middle:



Copyright © Albert R. Meyer, 2007. All rights reserved.

February 21, 2007

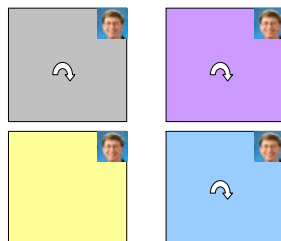
lec 3w.22

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

The Gehry/Gates Plaza

Method:

Rotate the squares as indicated.



Copyright © Albert R. Meyer, 2007. All rights reserved.

February 21, 2007

lec 3w.23

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

The Gehry/Gates Plaza

Method: after rotation have:



Copyright © Albert R. Meyer, 2007. All rights reserved.

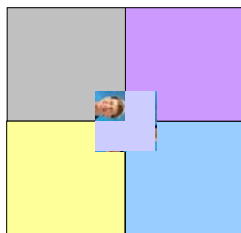
February 21, 2007

lec 3w.24



The Gehry/Gates Plaza

Method: Now group the 4 squares together, and insert a tile.



Done!
Bill in
middle

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 21, 2007

lec 3w.25



The Gehry/Gates Plaza

Theorem: For any $2^n \times 2^n$ plaza, we can put Bill in the corner.

Proof: (by induction on n)

$P(n) ::=$ can tile $2^n \times 2^n$ with Bill in corner

Base case: ($n=0$)



(no tiles needed)

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 21, 2007

lec 3w.26

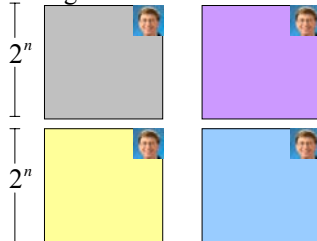


The Gehry/Gates Plaza

Induction step:

Assume we can get Bill in corner of $2^n \times 2^n$.

Prove we can get Bill in corner of $2^{n+1} \times 2^{n+1}$.



Copyright © Albert R. Meyer, 2007. All rights reserved.

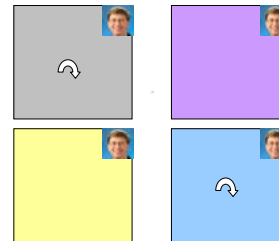
February 21, 2007

lec 3w.27



The Gehry/Gates Plaza

Method: Rotate the squares as indicated.



Copyright © Albert R. Meyer, 2007. All rights reserved.

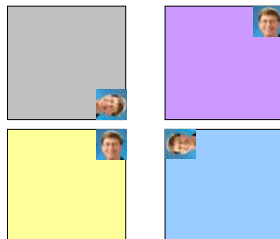
February 21, 2007

lec 3w.28



The Gehry/Gates Plaza

Method: Rotate the squares as indicated.
after rotation have:



Copyright © Albert R. Meyer, 2007. All rights reserved.

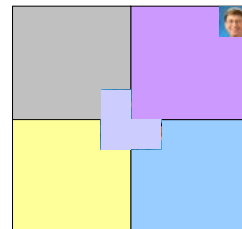
February 21, 2007

lec 3w.29



The Gehry/Gates Plaza

Method: Now group the squares together, and fill the center with a tile.



Done!

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 21, 2007

lec 3w.30

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

Ingenious Induction Hypotheses

Note 1: To prove
"Bill in middle," we
proved *something else*:
"Bill in corner."

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 21, 2007

lec 3w.31

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

Ingenious Induction Hypotheses

Note 2: It may help to
choose a stronger hypothesis
than the desired result
(class problem).

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 21, 2007

lec 3w.32

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

Recursive Procedure

Note 3: The induction proof
of "Bill in corner" implicitly
defines a *recursive procedure*
for finding corner tilings.

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 21, 2007

lec 3w.33

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

A False Proof

Theorem: All horses are the same color.

Proof: (by induction on n)

Induction hypothesis:

$P(n) ::=$ any set of n horses have the same color

Base case ($n=0$):

No horses so *vacuously* true!



Copyright © Albert R. Meyer, 2007. All rights reserved.

February 21, 2007

lec 3w.34

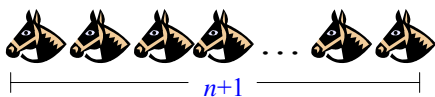
4	9	13	7
12		10	5
3	1	6	14
15	8	11	2

A False Proof

(Inductive case)

Assume any n horses have the same color.

Prove that any $n+1$ horses have the same color.



Copyright © Albert R. Meyer, 2007. All rights reserved.

February 21, 2007

lec 3w.35

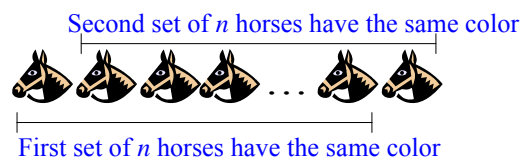
4	9	13	7
12		10	5
3	1	6	14
15	8	11	2

A False Proof

(Inductive case)

Assume any n horses have the same color.

Prove that any $n+1$ horses have the same color.



Copyright © Albert R. Meyer, 2007. All rights reserved.

February 21, 2007

lec 3w.36

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

A False Proof

(Inductive case)

Assume any n horses have the same color.
Prove that any $n+1$ horses have the same color.



Therefore the set of $n+1$ have the same color!

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 21, 2007

lec 3w.37

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

A False Proof

What is wrong? $n=1$

Proof that $P(n) \rightarrow P(n+1)$
is false if $n=1$, because the two
horse groups *do not overlap*.

Second set of $n=1$ horses



Copyright © Albert R. Meyer, 2007. All rights reserved.

February 21, 2007

lec 3w.38

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

A False Proof

Proof that $P(n) \rightarrow P(n+1)$
is false if $n=1$, because the two
horse groups *do not overlap*.

(But proof works for all $n \neq 1$)

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 21, 2007

lec 3w.39

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

Team Problems

Problems 1-3

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 21, 2007

lec 3w.40



Strong Induction Well Ordering Principle

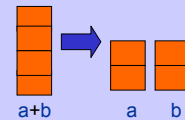
Copyright © Albert R. Meyer, 2007. All rights reserved.

February 23, 2007

lec 3f.1



Unstacking game



- Start: a stack of boxes
- Move: split any stack into two stacks of sizes $a, b > 0$
- Scoring: ab points
- Keep moving: until stuck
- Overall score: sum of move scores

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 23, 2007

lec 3f.2



Analyzing the Stacking Game

Claim: Every way of unstacking gives the same score.

From stack of size n , what score?

Must be

$$(n-1) + (n-2) + \dots + 1 = \frac{n(n-1)}{2}$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 23, 2007

lec 3f.3



Analyzing the Stacking Game

Claim: Starting with size n stack, final score will be

$$\frac{n(n-1)}{2}$$

Proof: by Induction with
Claim(n) as hypothesis

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 23, 2007


lec 3f.4



Proving the Claim by Induction

Base case $n = 0$:

$$\text{score} = 0 = \frac{0(0-1)}{2}$$

Claim(0) is 

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 23, 2007

lec 3f.5



Proving the Claim by Induction

Inductive step. assume for n -stack, and then prove *C*($n+1$):

$$(n+1)\text{-stack score} = \frac{(n+1)n}{2}$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 23, 2007

lec 3f.6

6	9	13	7
12		10	5
3	1	16	14
15	8	11	4

Proving the Claim by Induction

Inductive step.

Case $n+1 = 1$. verify for 1-stack:

$$\text{score} = 0 = \frac{1(1-1)}{2}$$

$C(1)$ is 

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 23, 2007

lec 3f.7

6	9	13	7
12		10	5
3	1	16	14
15	8	11	4

Proving the Claim by Induction

Inductive step.

Case $n+1 > 1$. So split into an a -stack and b -stack, where $a + b = n+1$.

$(a + b)$ -stack score = $ab + a$ -stack score + b -stack score

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 23, 2007

lec 3f.8

6	9	13	7
12		10	5
3	1	16	14
15	8	11	4

Proving the Claim by Induction

by induction:

$$a\text{-stack score} = \frac{a(a-1)}{2}$$

$$b\text{-stack score} = \frac{b(b-1)}{2}$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 23, 2007


lec 3f.9

6	9	13	7
12		10	5
3	1	16	14
15	8	11	4

Proving the Claim by Induction

total $(a + b)$ -stack score =

$$ab + \frac{a(a-1)}{2} + \frac{b(b-1)}{2} = \frac{(a+b)((a+b)-1)}{2} = \frac{(n+1)n}{2}$$

so $C(n+1)$ is 
We're done!

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 23, 2007

lec 3f.10

6	9	13	7
12		10	5
3	1	16	14
15	8	11	4

Proving the Claim by Induction

Wait: we assumed

$C(a)$ and $C(b)$

where $1 \leq a, b \leq n$.

But by induction

can only assume $C(n)$

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 23, 2007

lec 3f.11

6	9	13	7
12		10	5
3	1	16	14
15	8	11	4

Proving the Claim by Induction

the fix:

revise the induction hypothesis to

$Q(n) ::=$

$\forall m \leq n. C(m)$

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 23, 2007

lec 3f.12



Proving the Claim by Induction

Proof goes through fine using $Q(n)$ instead of $C(n)$.
So it's OK to assume $C(m)$ for all $m \leq n$ to prove $C(n+1)$.

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 23, 2007

lec 3f.13



Strong Induction

Prove $P(0)$. Then prove $P(n+1)$ assuming *all* of $P(0), P(1), \dots, P(n)$ (instead of just $P(n)$).

Conclude $\forall n. P(n)$

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 23, 2007

lec 3f.14



Strong vs. Ordinary

Why use Strong?
-- **Convenience:**
no need to include " $\forall m \leq n$ " all over.

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 23, 2007

lec 3f.17



Postage by Strong Induction

available stamps:



5¢

3¢

Theorem:

Can form any amount ≥ 8 ¢

Prove by **strong induction** on n .

$P(n) ::=$ can form $(n+8)$ ¢.

(Picture source: http://site17585.delhost.com/ig/facts/s_events.htm
<http://www.frbaf.org/currency/civilwar/stamps/s150.html>)

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 23, 2007

lec 3f.18



Postage by Strong Induction

Base case ($n = 0$):

$(0+8)$ ¢:



Copyright © Albert R. Meyer, 2007. All rights reserved.

February 23, 2007

lec 3f.19



Postage by Strong Induction

Inductive Step:

assume $(m+8)$ ¢ for $0 \leq m \leq n$,
then prove $((n+1)+8)$ ¢

cases:

$n+1 = 1, 9$ ¢:



$n+1 = 2, 10$ ¢:



Copyright © Albert R. Meyer, 2007. All rights reserved.

February 23, 2007

lec 3f.20



Postage by Strong Induction

case $n+1 \geq 3$: let $m = n - 2$.

now $n \geq m \geq 0$, so

by induction hypothesis have:

$$\text{cloud} + 3 = (n+1)+8$$

|— $(n-2)+8$ —|

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 23, 2007

lec 3f.21



Team Problem

Problem 1

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 23, 2007

lec 3f.22



Well Ordering Principle

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 23, 2007

lec 3f.23



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:**

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 23, 2007

lec 3f.24



Well Ordering principle

Every nonempty set of

nonnegative **rational**s

has a

least element.

NO!

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 23, 2007

lec 3f.25



Well Ordering principle

Every nonempty set of

~~nonnegative~~ *integers*

has a

least element.

NO!

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 23, 2007

lec 3f.26



$\sqrt{2}$ proof used Well Ordering

Thm: $\sqrt{2}$ is irrational

Proof: suppose $\sqrt{2} = \frac{m}{n}$

...can **always** find such m, n
without common factors...

why always?

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 23, 2007

lec 3f.27



Proof using Well Ordering

By **WOP**, \exists **minimum** $|m|$ s.t.

$$\sqrt{2} = \frac{m}{n}. \quad \text{so} \quad \sqrt{2} = \frac{m_0}{n_0}$$

where $|m_0|$ is **minimum**.

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 23, 2007

lec 3f.28



Proof using Well Ordering

but if m_0, n_0 had common factor $c > 1$, then

$$\sqrt{2} = \frac{m_0 / c}{n_0 / c}$$

and $|m_0 / c| < |m_0|$
contradicting minimality of $|m_0|$

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 23, 2007

lec 3f.29



Well Ordering Principle Proofs

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

- Define the set of *counterexamples*
 $C ::= \{n \in \mathbb{N} \mid \neg P(n)\}$
- Assume C is not empty.
- By WOP, have minimum element $m_0 \in C$.
- Reach a contradiction (*somehow*) – usually by finding a member of C that is $< m_0$.
- Conclude no counterexamples exist. QED

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 23, 2007

lec 3f.33



Team Problem

Problem 2

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 23, 2007

lec 3f.34

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

Recursive Definitions Structural Induction

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

Recursive Definitions

Define something in terms of a simpler version of the same thing:

- **Base case(s)** that don't depend on anything else.
- **Constructor case(s)** that depend on simpler cases.

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

Example Definition: set E

Define set $E \subseteq \mathbb{Z}$, recursively:

- **Base case:** $0 \in E$
- **Constructor cases:**

If $n \in E$, then

1. $n + 2 \in E$, if $n \geq 0$;
2. $-n \in E$, if $n > 0$.

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

Example Definition: set E

1. $n \in E$ and $n \geq 0$, then $n + 2 \in E$:

0, 0+2, (0+2)+2, ((0+2)+2)+2

0, 2, 4, 6, ...

2. $n \in E$ and $n > 0$, then $-n \in E$

-2, -4, -6, ...

all even numbers

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

Recursive Definition: Extremal Clause

So, E contains the even integers
Anything Else? **No!**

- $0 \in E$
- If $n \in E$ and $n \geq 0$, then $n + 2 \in E$
- If $n \in E$ and $n > 0$, then $-n \in E$
- **That's All!**

Extremal Clause

(Implicit part of definition)

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

Example Definition: set E

So E is **exactly**:
The Even Integers

6	9	13	7
12	10	5	
3	4	14	15
16	8	11	2

Example: Matched Paren Strings, M

Set of strings, $M \subseteq \{ \}, \{ \}^*$

- **Base:** $\lambda \in M$,
(the *empty string*)

- **Constructor:**

If $s, t \in M$, then

$$(s)t \in M$$

Copyright © Albert R. Meyer, 2007. All rights reserved. February 26, 2007

lec 4M-7

6	9	13	7
12	10	5	
3	4	14	15
16	8	11	2

Example: Matched Paren Strings, M

Lemma: Every s in M has an equal number of $)$'s and $($'s.

Proof by **Structural Induction** on the definition of M

Copyright © Albert R. Meyer, 2007. All rights reserved. February 26, 2007

lec 4M-8

6	9	13	7
12	10	5	
3	4	14	15
16	8	11	2

Example: Matched Paren Strings, M

Lemma: Every s in M has an equal number of $)$'s and $($'s.

Let $EQ ::=$
{strings with = number of $)$ and $($ }

Lemma (restated): $M \subseteq EQ$

Copyright © Albert R. Meyer, 2007. All rights reserved. February 26, 2007

lec 4M-9

6	9	13	7
12	10	5	
3	4	14	15
16	8	11	2

Structural Induction on M

Proof:

Hypothesis $P(s) ::= s \in EQ$

Base case: $s = \lambda$. $P(\lambda)$?
0 $)$'s and 0 $($'s. **OK**

Copyright © Albert R. Meyer, 2007. All rights reserved. February 26, 2007

lec 4M-10

6	9	13	7
12	10	5	
3	4	14	15
16	8	11	2

Structural Induction on M

Constructor step

$r = (s)t$. Assume: $P(s)$ and $P(t)$

$$\begin{aligned} \#) \text{ in } r &= \#) \text{ in } s + \#) \text{ in } t + 1 \\ \#(\text{ in } r &= \#(\text{ in } s + \#(\text{ in } t + 1 \\ \therefore \text{ are } &= \text{ by } P(s) = \text{ by } P(t) \end{aligned}$$

Copyright © Albert R. Meyer, 2007. All rights reserved. February 26, 2007

lec 4M-11

6	9	13	7
12	10	5	
3	4	14	15
16	8	11	2

Structural Induction on M

by structural induction,

$$\forall s \in M. s \in EQ$$

QED

Copyright © Albert R. Meyer, 2007. All rights reserved. February 26, 2007

lec 4M-12

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

The 18.01 Functions, F18

The set F18 of functions on \mathbb{R} :

- $\text{Id}_{\mathbb{R}}$, constant functions, and $\sin x$ are in F18.
- if $f, g \in \text{F18}$, then
 - $f + g$, $f \cdot g$, e^f , (the constant e)
 - the inverse, $f^{(-1)}$, of f , and
 - $f \circ g$ (the composition of f and g) are in F18.

Copyright © Albert R. Meyer, 2007. All rights reserved. February 26, 2007

lec 4M-13

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

The 18.01 Functions, F18

Some functions in F18:

$$\begin{aligned} -x &= (-1) \cdot x \\ \sqrt{x} &= (x^2)^{(-1)} \text{ ---inverse} \\ \cos x &= (1 - (\sin x \cdot \sin x))^{1/2} \\ \ln x &= (e^x)^{(-1)} \end{aligned}$$

Copyright © Albert R. Meyer, 2007. All rights reserved. February 26, 2007

lec 4M-14

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

The 18.01 Functions, F18

Lemma. F18 is *closed under derivative*:
if $f \in \text{F18}$, then $f' \in \text{F18}$.

(Team problem 2)

Copyright © Albert R. Meyer, 2007. All rights reserved. February 26, 2007

lec 4M-15

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

Recursive Data Types

Arithmetic Expressions

Copyright © Albert R. Meyer, 2007. All rights reserved. February 26, 2007

lec 4M-19

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

Arithmetic Expressions

Defined recursively as follows:

Base:

- if $n \in \mathbb{N}$, then $\langle \text{int}, n \rangle \in \text{Aexp}$
- if $n \in \mathbb{N}$, then $\langle \text{var}, n \rangle \in \text{Aexp}$

“tagged” data

Copyright © Albert R. Meyer, 2007. All rights reserved. February 26, 2007

lec 4M-20

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

Arithmetic Expressions

Constructors:

if $e, f \in \text{Aexp}$, then

1. $\langle \text{sum}, e, f \rangle \in \text{Aexp}$
2. $\langle \text{prod}, e, f \rangle \in \text{Aexp}$

Copyright © Albert R. Meyer, 2007. All rights reserved. February 26, 2007

lec 4M-21

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

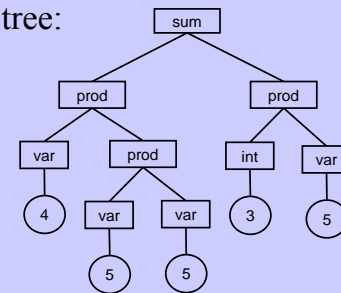
$$x_4(x_5)^2 + 3x_5$$

<sum, <prod,
 <var, 4>,
 <prod, <var, 5>, <var, 5>>
 >,
 <prod, <int, 3>, <var, 5>>
 >

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

$$x_4(x_5)^2 + 3x_5$$

Parse tree:



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

Recursive Functions on Aexp

Recursive def. of *size*, $|e|$, of e

$|\langle \text{int}, n \rangle| ::= 1$
 $|\langle \text{var}, n \rangle| ::= 1$
 $|\langle \text{sum}, e, f \rangle| ::= |e| + |f| + 1$
 $|\langle \text{prod}, e, f \rangle| ::= |e| + |f| + 1$

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

Recursive Functions on Aexp

Recursive def. of *depth*, $d(e)$

$d(\langle \text{int}, n \rangle) ::= 0$
 $d(\langle \text{var}, n \rangle) ::= 0$
 $d(\langle \text{sum}, e, f \rangle) ::= 1 + \max\{d(e), d(f)\}$
 $d(\langle \text{prod}, e, f \rangle) ::= 1 + \max\{d(e), d(f)\}$

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

Size versus Depth

Lemma: $|e| + 1 \leq 2^{d(e)+1}$

Proof by **Structural Induction**

Base case: $e = \langle \text{int}, n \rangle$ (or $\langle \text{var}, n \rangle$)

$$|e| + 1 = 1 + 1 = 2 = 2^{0+1} = 2^{d(e)+1}$$

OK!

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

Size versus Depth

Constructor case: $e = \langle \text{sum}, e_1, e_2 \rangle$

by ind. hypothesis:

$$|e_i| + 1 \leq 2^{d(e_i)+1} \quad i=1,2$$

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

Size versus Depth

$$\begin{aligned}
 |e| + 1 &= |\langle \text{sum}, e_1, e_2 \rangle| + 1 && \text{def. of } e \\
 &= (|e_1| + |e_2| + 1) + 1 && \text{def. of size} \\
 &= (|e_1| + 1) + (|e_2| + 1) \\
 &\leq 2^{d(e_1)+1} + 2^{d(e_2)+1} && \text{induction hyp.} \\
 &\leq 2^{\max(d(e_1), d(e_2))+1} + 2^{\max(d(e_1), d(e_2))+1} \\
 &= 2^{(\max(d(e_1), d(e_2))+1)+1} = 2^{d(e)+1} && \text{def. of depth} \\
 &\quad \text{QED}
 \end{aligned}$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 26, 2007

lec 4M-28

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

Team Problems

Problems 1--3

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 26, 2007

lec 4M-29



State Machines, I: Invariants

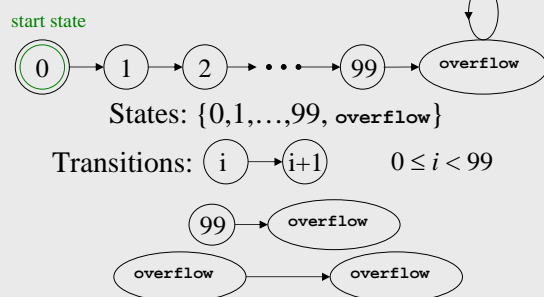


State machine:

Step by step procedure,
possibly responding to input.



The **state graph** of a 99-bounded counter:



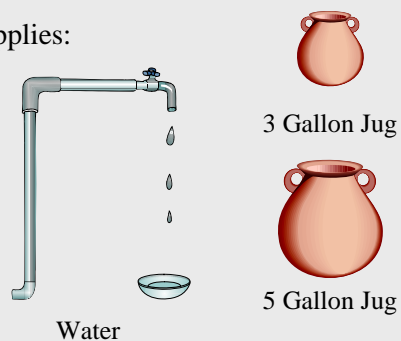
Picture source: <http://movieweb.com/movie/diehard3/>



Simon says: On the fountain, there should be 2 jugs, do you see them? A 5-gallon and a 3-gallon. Fill one of the jugs with exactly 4 gallons of water and place it on the scale and the timer will stop. You must be precise; one ounce more or less will result in detonation. If you're still alive in 5 minutes, we'll speak.



Supplies:





Die Hard

Transferring water:



3 Gallon Jug

5 Gallon Jug

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 28, 2007

lec 4W.7



Die Hard

Transferring water:



3 Gallon Jug

5 Gallon Jug

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 28, 2007

lec 4W.8



Die Hard

Simon's challenge:

Disarm the bomb by putting
precisely 4 gallons of water on
the scale, or it will **blow up**.

Question: How to do it?

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 28, 2007

lec 4W.9



Die Hard

Work it out now!

Copyright © Albert R. Meyer, 2007. All rights reserved.

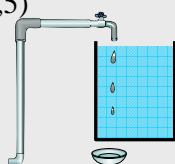
February 28, 2007

lec 4W.10



How to do it

Start with empty jugs: (0,0)
Fill the big jug: (0,5)



3 Gallon Jug

5 Gallon Jug

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 28, 2007

lec 4W.11



How to do it

Pour from big to little: (3,2)



3 Gallon Jug

5 Gallon Jug

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 28, 2007

lec 4W.12

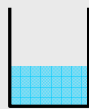
1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

How to do it

Empty the little: (0,2)



3 Gallon Jug



5 Gallon Jug

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 28, 2007

lec 4W.13

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

How to do it

Pour from big to little: (2,0)



3 Gallon Jug



5 Gallon Jug

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 28, 2007

lec 4W.14

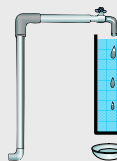
1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

How to do it

Fill the big jug: (2,5)



3 Gallon Jug



5 Gallon Jug

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 28, 2007

lec 4W.15

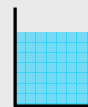
1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

How to do it

Pour from big to little: (3,4)



3 Gallon Jug



5 Gallon Jug

Done!!

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 28, 2007

lec 4W.16

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Die Hard **once and for all**

What if you have a 9 gallon jug instead?



3 Gallon Jug



~~5 Gallon Jug~~



9 Gallon Jug

Can you do it? Can you prove it?

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 28, 2007

lec 4W.17

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Die Hard

Work it out now!

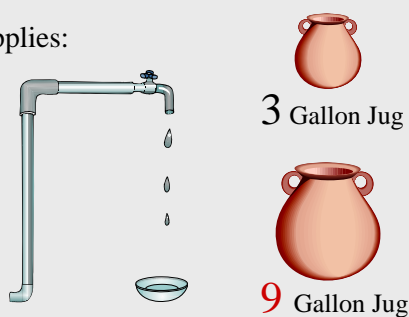
Copyright © Albert R. Meyer, 2007. All rights reserved.

February 28, 2007

lec 4W.18

Die Hard Once & For All

Supplies:



Water

Copyright © Albert R. Meyer, 2007. All rights reserved. February 28, 2007 lec 4W.19

State machines

Die hard state machine

State = amount of water in the jug: (b, l)
 where $0 \leq b \leq 9$ and $0 \leq l \leq 3$.
 Start State = $(0, 0)$

Copyright © Albert R. Meyer, 2007. All rights reserved. February 28, 2007 lec 4W.20

State machines

Die Hard Transitions:

1. Fill the little jug: $(b, l) \rightarrow (b, 3)$ for $l < 3$
2. Fill the big jug: $(b, l) \rightarrow (9, l)$ for $b < 9$
3. Empty the little jug: $(b, l) \rightarrow (b, 0)$ for $l > 0$
4. Empty the big jug: $(b, l) \rightarrow (0, l)$ for $b > 0$

Copyright © Albert R. Meyer, 2007. All rights reserved. February 28, 2007 lec 4W.21

State machines

5. Pour from big jug into little jug (for $b > 0$):
 - (i) If no overflow, then $(b, l) \rightarrow (0, b+l)$,
 $b + l \leq 3$
 - (ii) otherwise $(b, l) \rightarrow (b - (3 - l), 3)$.
6. Pour from little jug into big jug.
 Likewise.

Copyright © Albert R. Meyer, 2007. All rights reserved. February 28, 2007 lec 4W.22

State Invariants

Die hard once and for all

Invariant:

$P(\text{state}) ::= \text{"3 divides the number of gallons in each jug."}$

$P((b, l)) ::= (3 \mid b \wedge 3 \mid l)$


Copyright © Albert R. Meyer, 2007. All rights reserved. February 28, 2007 lec 4W.23

State Invariants

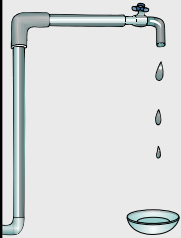
Floyd's Invariant Method
 (just like induction)

- 1) **Base case:** Show $P(\text{start})$.
- 2) **Invariant case:** Show
 if $P(q)$ and $q \rightarrow r$, then $P(r)$.
- 3) **Conclusion:** P holds for all reachable states, including final state (if any).

Copyright © Albert R. Meyer, 2007. All rights reserved. February 28, 2007 lec 4W.24




Die Hard Once & For All



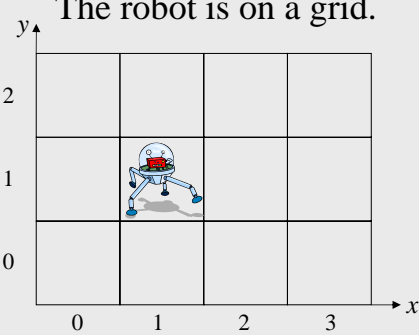
Corollary: No state $(4,x)$ is reachable, so **Bruce Dies!**

Copyright © Albert R. Meyer, 2007. All rights reserved. February 28, 2007 lec 4W.25




The Diagonal Robot

The robot is on a grid.

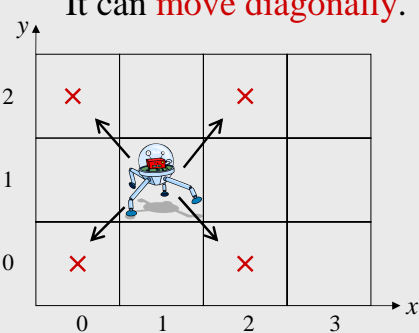


Copyright © Albert R. Meyer, 2007. All rights reserved. February 28, 2007 lec 4W.26




The Diagonal Robot

It can **move diagonally**.




Copyright © Albert R. Meyer, 2007. All rights reserved. February 28, 2007 lec 4W.27




The Diagonal Robot

Can it reach from $(0,0)$ to $(1,0)$?



Copyright © Albert R. Meyer, 2007. All rights reserved. February 28, 2007 lec 4W.28




Robot Invariant

NO!

$P((x, y)) ::= x + y$ is even
is an invariant:
transition adds ± 1 to **both** x and y ,
preserving parity of $x+y$.
Also, $P((0, 0))$ is true.

Copyright © Albert R. Meyer, 2007. All rights reserved. February 28, 2007 lec 4W.29



Robot Invariant

So all positions (x, y) reachable
by robot have $x + y$ **even**.

But $1 + 0 = 1$ is **odd**, so
 $(1,0)$ is not reachable.

Copyright © Albert R. Meyer, 2007. All rights reserved. February 28, 2007 lec 4W.30

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

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

The Fifteen Puzzle Explained!

--by similar reasoning
(details in Team Problem 1)

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 28, 2007

lec 4W.31

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

Team Problems

Problems carried
over to Friday

Copyright © Albert R. Meyer, 2007. All rights reserved.

February 28, 2007

lec 4W.32



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

The Fifteen Puzzle Explained!

Wednesday,
Team Problem 1

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 2, 2007

lec 4F.1



Mathematics for Computer Science

MIT 6.042J/18.062J

State Machine Invariants, cont'd

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 2, 2007

lec 4F.2



GCD correctness

The Euclidean Algorithm:

Computing $\text{GCD}(a, b)$

1. $x := a, y := b.$
2. If $y = 0$, return x & terminate; else
3. $(x, y) := (y, \text{rem}(x, y))$
simultaneously;
4. Go to step 2.

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 2, 2007

lec 4F.3



GCD correctness

Example: $\text{GCD}(414, 662)$

$= \text{GCD}(662, 414)$ since $\text{rem}(414, 662) = 414$
 $= \text{GCD}(414, 248)$ since $\text{rem}(662, 414) = 248$
 $= \text{GCD}(248, 166)$ since $\text{rem}(414, 248) = 166$
 $= \text{GCD}(166, 82)$ since $\text{rem}(248, 166) = 82$
 $= \text{GCD}(82, 2)$ since $\text{rem}(166, 82) = 2$
 $= \text{GCD}(2, 0)$ since $\text{rem}(82, 2) = 0$

Return value: 2.

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 2, 2007

lec 4F.4



GCD correctness

Euclid Algorithm as State Machine:

- States $::= \mathbb{N} \times \mathbb{N}$,
- start $::= (a, b)$,
- state transitions defined by the rule
 $(x, y) \rightarrow (y, \text{rem}(x, y))$ for $y \neq 0$.

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 2, 2007

lec 4F.5



GCD correctness

The Invariant is

$P((x, y)) ::= [\text{gcd}(a, b) = \text{gcd}(x, y)].$

$P(\text{start})$: at start $x = a, y = b$, so

$P(\text{start}) \equiv [\text{gcd}(a, b) = \text{gcd}(a, b)]$
which holds trivially.

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 2, 2007

lec 4F.6

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

GCD correctness

Transitions: $(x, y) \rightarrow (y, \text{rem}(x, y))$

Invariant holds by

Lemma: $\text{gcd}(x, y) = \text{gcd}(y, \text{rem}(x, y))$,
for $y \neq 0$.

Proof: $x = qy + \text{rem}$, so
any divisor of x, y divides rem ;
any divisor of y, rem divides x

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 2, 2007

lec 4F.7

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

GCD correctness

Conclusion: on termination

$$x = \text{gcd}(a, b).$$

Proof: at termination, $y = 0$, so
 $x = \text{gcd}(x, 0) = \underbrace{\text{gcd}(x, y) = \text{gcd}(a, b)}_{\text{the invariant}}$

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 2, 2007

lec 4F.8

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

GCD Termination

y decreases at each step &
 $y \in \mathbb{N}$ (another invariant).

Well Ordering implies
reaches minimum & stops.

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 2, 2007

lec 4F.9

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

Robert W Floyd (1934–2001)



Eulogy by Knuth: <http://www.acm.org/pubs/membernet/stories/floyd.pdf>
Picture source: <http://www.stanford.edu/dept/news/report/news/november7/floydobit-117.html>

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 2, 2007

lec 4F.10

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

Mathematics for Computer Science

MIT 6.042J/18.062J

State Machines: Derived Variables

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 2, 2007

lec 4F.11

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

Derived Variables

A *derived variable*, v , is a function
giving a “value” to each state:

$$v: Q \rightarrow \text{Values}.$$

If $\text{Values} = \mathbb{N}$, we’d say v was

“nonnegative-integer-valued,” or
“ \mathbb{N} -valued.”

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 2, 2007

lec 4F.12

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

Derived Variables

Robot on the grid example:

States $Q = \mathbb{N}^2$.

Define the sum-value, σ , of a state:

$$\sigma(\langle x, y \rangle) ::= x + y$$

An \mathbb{N} -valued derived variable.

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 2, 2007

lec 4F:13

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

Derived Variables

Called “**derived**” to distinguish from **actual** variables that appear in a program.

For robot **Actual:** x, y

Derived: σ

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 2, 2007

lec 4F:14

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

Derived Variables

Another derived variable:

$$\pi ::= \sigma \pmod{2}.$$

π is $\{0, 1\}$ -valued.

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 2, 2007

lec 4F:15

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

Derived Variables

For GCD, have (actual) variables x, y .

Proof of **GCD termination**:

y is **strictly decreasing** and **natural number-valued**.

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 2, 2007

lec 4F:16

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

Derived Variables

Termination followed by

Well Ordering Principle:

y must take a **least value** – and then the algorithm is stuck.

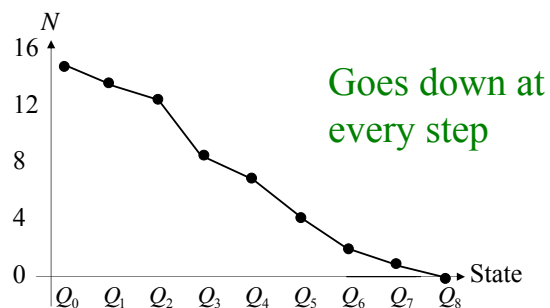
Copyright © Albert R. Meyer, 2007. All rights reserved.

March 2, 2007

lec 4F:17

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

Strictly Decreasing Variable



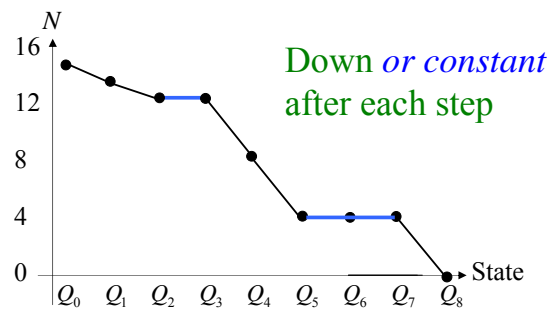
Copyright © Albert R. Meyer, 2007. All rights reserved.

March 2, 2007

lec 4F:18

4	9	13	7
12	6	10	5
3	1	14	11
15	8	16	2

Weakly Decreasing Variable



Copyright © Albert R. Meyer, 2007. All rights reserved.

March 2, 2007

lec 4F.19

4	9	13	7
12	6	10	5
3	1	14	11
15	8	16	2

σ , π for the Diagonal Robot

σ : up & down all over the place –
neither increasing nor decreasing.
 π : is constant –
both increasing & decreasing
(weakly)

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 2, 2007

lec 4F.20

4	9	13	7
12	6	10	5
3	1	14	11
15	8	16	2

Partial-order valued variables

Definitions of increasing/decreasing variables extend to variables with partially ordered values.
If a partial order has no infinite, decreasing chain (it is *well-founded*), then it can serve instead of \mathbb{N} to
prove termination.

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 2, 2007

lec 4F.23

4	9	13	7
12	6	10	5
3	1	14	11
15	8	16	2

Team Problems

Wednesday, Problem 2;
and today's
Problems 1& 2

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 2, 2007

lec 4F.24

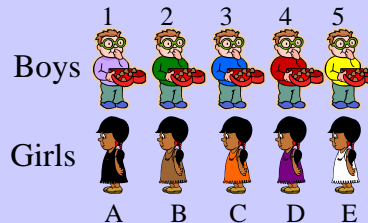


Stable Matching



Stable Marriage

A Marriage Problem



Stable Marriage

Preferences:

Boys	Girls
1: CBEAD	A: 35214
2: ABECD	B: 52143
3: DCBAE	C: 43512
4: ACDBE	D: 12345
5: ABDEC	E: 23415



Stable Marriage

Preferences

1: CBEAD
2: ABECD
3: DCBAE
4: ACDBE
5: ABDEC

Try “greedy”
strategy for boys



Stable Marriage

Preferences

1: C BEAD
2: ABE C D
3: D C BAE
4: A C DBE
5: ABDE C

Marry Boy 1 with Girl C
(his 1st choice)




Stable Marriage

Preferences

2: ABE D
3: D BAE
4: A DBE
5: ABDE

Marry Boy 1 with Girl C
(his 1st choice)












Stable Marriage

Preferences


Marry **Boy 1** with **Girl C**
(his 1st choice)


2 : ABED

3 : DBAE

4 : ADBE

5 : ABDE

1C






Copyright © Albert R. Meyer, 2007. All rights reserved. March 5, 2007 lec 5M.7






Stable Marriage

Next:


Marry **Boy 2** with **Girl A**:
(best remaining choice)

 C
 ~~2 : ABED~~
 3 : DBAE
 4 : ~~ADBE~~
 5 : ~~ABDE~~




2A

Copyright © Albert R. Meyer, 2007. All rights reserved. March 5, 2007 lec 5M.8






Stable Marriage




Final “boy greedy” marriages




1 C




2 A

3 D






4 B




5 E

Copyright © Albert R. Meyer, 2007. All rights reserved. March 5, 2007 lec 5M.9






Stable Marriage

Trouble!






1C




4B

Copyright © Albert R. Meyer, 2007. All rights reserved. March 5, 2007 lec 5M.10






Stable Marriage

Boy 4 **likes** Girl C **better** than his wife.


1C

4B




(Dashed red arrow from Boy 4 to Girl C with a heart icon)

Copyright © Albert R. Meyer, 2007. All rights reserved. March 5, 2007 lec 5M.11






Stable Marriage

and vice-versa


1C

4B

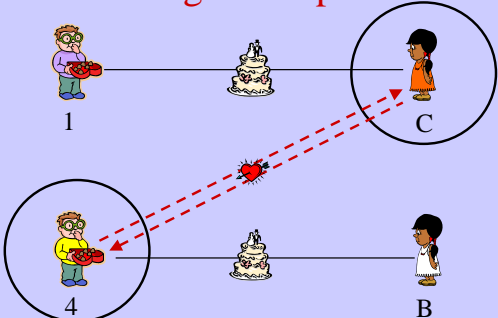
(Dashed red arrow from Girl C to Boy 4 with a heart icon)

Copyright © Albert R. Meyer, 2007. All rights reserved. March 5, 2007 lec 5M.12



Stable Marriage


Rogue Couple



1 C

4 B


Copyright © Albert R. Meyer, 2007. All rights reserved. March 5, 2007 lec 5M.13



Stable Marriage

Stable Marriage Problem:
Marry everyone without
any rogue couples!


Copyright © Albert R. Meyer, 2007. All rights reserved. March 5, 2007 lec 5M.14



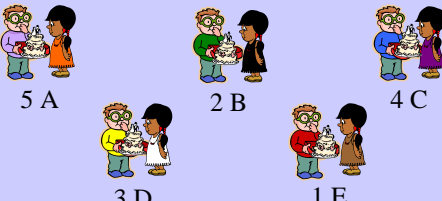
Stable Marriage

Let's Try it!
Unnumbered Class
Problem

Copyright © Albert R. Meyer, 2007. All rights reserved. March 5, 2007 lec 5M.15



Stable Marriage I.




5 A 2 B 4 C

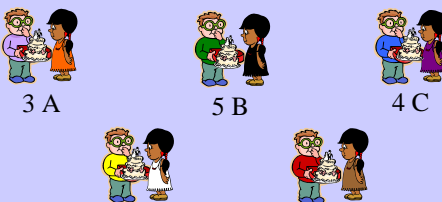
3 D 1 E

Boy Optimal

Copyright © Albert R. Meyer, 2007. All rights reserved. March 5, 2007 lec 5M.17



Stable Marriage II.




3 A 5 B 4 C

1 D 2 E

All Girls get 1st Choice

Copyright © Albert R. Meyer, 2007. All rights reserved. March 5, 2007 lec 5M.18



Stable Marriage

More than a puzzle:

- College Admissions
(original Gale & Shapley paper, 1962)
- Matching Hospitals & Residents.
- Matching Dance Partners.

Copyright © Albert R. Meyer, 2007. All rights reserved. March 5, 2007 lec 5M.19



Stable Marriage



Copyright © Albert R. Meyer, 2007. All rights reserved.

March 5, 2007

lec 5M.20



Stable Marriage

The Mating Ritual:
day by day

Copyright © Albert R. Meyer, 2007. All rights reserved.

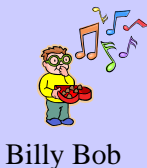
March 5, 2007

lec 5M.21



Mating Ritual

Morning: boy serenades favorite girl



Billy Bob



Brad



Angelina

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 5, 2007

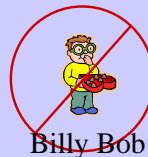
lec 5M.22



Mating Ritual

Morning: boy serenades favorite girl

Afternoon: girl **rejects** all but favorite



Billy Bob



Brad



Angelina

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 5, 2007

lec 5M.23



Mating Ritual

Morning: boy serenades favorite girl

Afternoon: girl rejects all but favorite

Evening: rejected boy writes off girl



Billy Bob



Copyright © Albert R. Meyer, 2007. All rights reserved.

March 5, 2007

lec 5M.24



Mating Ritual

Stop when no girl rejects.

Each girl marries her favorite
suitor (if any).

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 5, 2007

lec 5M.25

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Mating Ritual

Partial Correctness:

- Everyone is married.
- Marriages are stable.

Termination:

there exists a Wedding Day.

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 5, 2007

lec 5M.26

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Stable Marriage: Termination

total-boy's-list-length:
strictly decreasing & \mathbb{N} -valued.

So \exists Wedding Day.

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 5, 2007

lec 5M.27

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Mating Ritual: Girls improve

Lemma: A girl's favorite tomorrow will be at least as desirable as today's.

...because today's favorite will stay until she rejects him for someone better.

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 5, 2007

lec 5M.30

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Mating Ritual: Girls improve

Lemma: A girl's favorite tomorrow will be at least as desirable as today's.

(*favorite*(G) is **weakly increasing** for each G)

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 5, 2007

lec 5M.31

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Mating Ritual: Boys Get Worse

Lemma: A boy's 1st love tomorrow will be no more desirable than today's.

...because boys work straight down their lists.

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 5, 2007

lec 5M.32

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Mating Algorithm: Boys Get Worse

Lemma: A boy's 1st love tomorrow will be no more desirable than today's.

(*serenading*(B) is **weakly decreasing** for each B)

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 5, 2007

lec 5M.33

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Mating Ritual: **Invariant**

If G is not on B 's list, then she has a better current favorite.

Proof: When G rejected B she had a better suitor, and $favorite(G)$ is weakly increasing.

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 5, 2007

lec 5M.34

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Stable Marriage: Termination

On Wedding Day:

- Each girl has ≤ 1 suitors
(by def of wedding day)
- Each boy is married, or has no girls on his list

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 5, 2007

lec 5M.35

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Mating Ritual: Everyone Marries

Everyone is Married by Wedding Day

Proof: by **contradiction**.

If B is not married, his list is empty.

By **Invariant**, all girls have favorites better than B -- so they *do* have a favorite.

That is, all **girls** are married, so all **boys** are married.

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 5, 2007

lec 5M.36

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Mating Ritual: Stable Marriages

Marriages are **Stable**:

Bob won't be in rogue couple with

case 1: a girl G **on** his final list, since **he's already married to the best of them**.

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 5, 2007

lec 5M.37

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Mating Ritual: Stable Marriages

Marriages are **Stable**:

Bob won't be in rogue couple with

case 2: a girl G **not on** his final list, since **by Invariant**, G likes her spouse better.

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 5, 2007

lec 5M.38

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Mating Ritual

Who does better, boys or girls?

Girls' suitors get better, and boy's sweethearts get worse, so girls do better?

No!

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 5, 2007

lec 5M.39

6	9	13	7
12		10	5
3	1	16	15
14	8	11	4

Mating Ritual

Mating Ritual is *Optimal* for all Boys at once. *Pessimal* for all Girls.

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 5, 2007

lec 5M.40

6	9	13	7
12		10	5
3	1	16	15
14	8	11	4

Stable Marriage

More questions, rich theory:

Other stable marriages possible?

- Can be many.

Can a boy do better by lying? – No!

Can a girl do better by lying? – Yes!

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 5, 2007

lec 5M.41

6	9	13	7
12		10	5
3	1	16	15
14	8	11	4

Team Problems

Problems

1–3

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 5, 2007

lec 5M.42



Mathematics for Computer Science

MIT 6.042J/18.062J

Simple Graphs: Degrees, Isomorphism, Paths

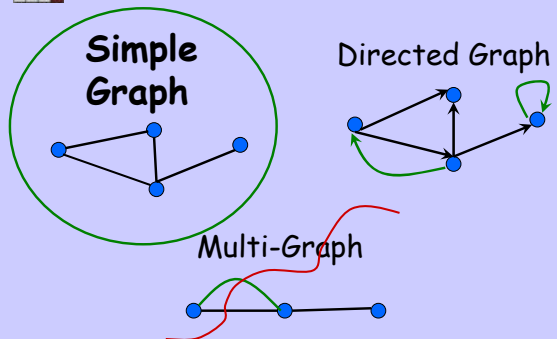
Copyright © Albert R. Meyer, 2007. All rights reserved.

March 7, 2007

lec 5W.1



Types of Graphs



Copyright © Albert R. Meyer, 2007. All rights reserved.

March 7, 2007

lec 5W.2



A Simple Graph

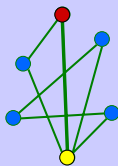
vertices, V

undirected edges, E

$::= \{ \bullet, \bullet \}$

"adjacent"

edge



Copyright © Albert R. Meyer, 2007. All rights reserved.

March 7, 2007

lec 5W.3



Vertex Degree

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 7, 2007

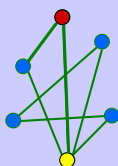
lec 5W.4



Vertex degree

degree of a vertex is
of *incident* edges

$$\deg(\bullet) = 2$$



Copyright © Albert R. Meyer, 2007. All rights reserved.

March 7, 2007

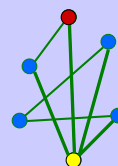
lec 5W.5



Vertex degree

degree of a vertex is
of *incident* edges

$$\deg(\bullet) = 4$$



Copyright © Albert R. Meyer, 2007. All rights reserved.

March 7, 2007

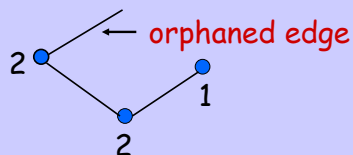
lec 5W.6

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

Impossible Graph

Is there a graph with
vertex degrees 2,2,1?

NO!



Copyright © Albert R. Meyer, 2007. All rights reserved.

March 7, 2007

lec 5W.7

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

Handshaking Lemma

sum of degrees is
twice # edges

$$2|E| = \sum_{v \in V} \deg(v)$$

$2+2+1 = \text{odd}$,
so impossible

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 7, 2007

lec 5W.8

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

Handshaking Lemma

sum of degrees is
twice # edges

$$2|E| = \sum_{v \in V} \deg(v)$$

Proof: Each edge contributes
2 to the sum on the right

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 7, 2007

lec 5W.9

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

Sex in America: Men more Promiscuous?

Study claims:

**Men average many more
partners than women.**

Graph theory shows
this is nonsense

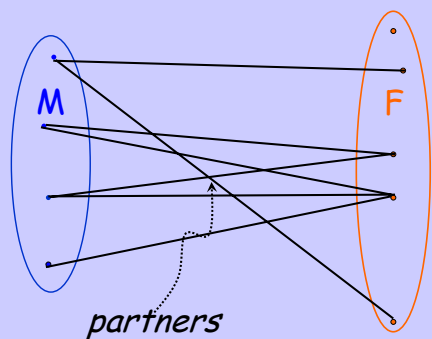
Copyright © Albert R. Meyer, 2007. All rights reserved.

March 7, 2007

lec 5W.10

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

Sex Partner Graph



Copyright © Albert R. Meyer, 2007. All rights reserved.

March 7, 2007

lec 5W.11

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

Counting pairs of partners

$$\sum_{m \in M} \deg(m) = |E| = \sum_{f \in F} \deg(f)$$

divide by both sides by $|M|$

$$\underbrace{\frac{\sum_{m \in M} \deg(m)}{|M|}}_{\text{avg-deg}(M)} = \underbrace{\frac{\sum_{f \in F} \deg(f)}{|F|}}_{\text{avg-deg}(F)} \frac{|F|}{|M|}$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 7, 2007

lec 5W.12

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

Average number of partners

$$(\text{avg-deg}(M)) = (\text{avg-deg}(F)) 1.035$$

Averages differ solely by
ratio of females to males.

No big difference
Nothing to do with promiscuity.

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 7, 2007

lec 5W.13

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

Isomorphism

Copyright © Albert R. Meyer, 2007. All rights reserved.

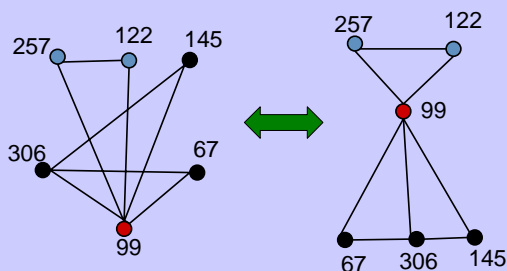
March 7, 2007

lec 5W.14

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

The Graph Abstraction

Same graph (different *layouts*)



Copyright © Albert R. Meyer, 2007. All rights reserved.

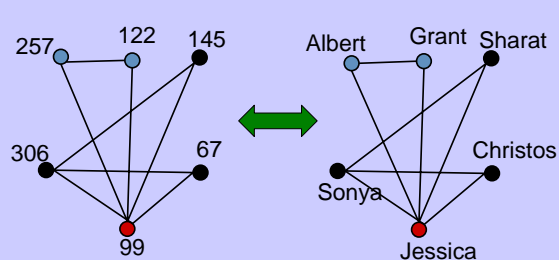
March 7, 2007

lec 5W.15

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

The Graph Abstraction

Same graph (different *labels*)



Copyright © Albert R. Meyer, 2007. All rights reserved.

March 7, 2007

lec 5W.16

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

The Graph Abstraction

All that matters
is the *connections*.
Graphs with the
same connections
are *isomorphic*.

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 7, 2007

lec 5W.17

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


Isomorphism

G_1 *isomorphic* to G_2 means
there is an *edge-preserving*
vertex matching.

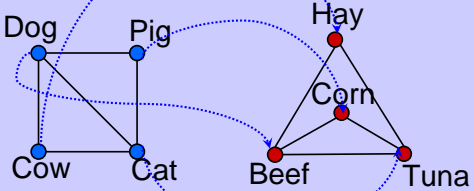
Copyright © Albert R. Meyer, 2007. All rights reserved.

March 7, 2007

lec 5W.18




Are these Isomorphic?

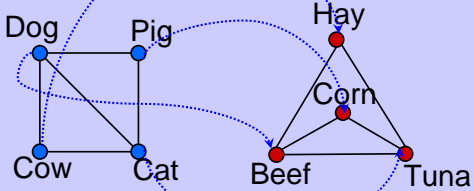


$f(\text{Dog}) = \text{Beef}$ $f(\text{Cow}) = \text{Hay}$
 $f(\text{Cat}) = \text{Tuna}$ $f(\text{Pig}) = \text{Corn}$


Copyright © Albert R. Meyer, 2007. All rights reserved. March 7, 2007 lec 5W.19



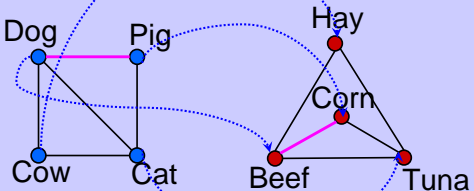
Edges Preserved?




Copyright © Albert R. Meyer, 2007. All rights reserved. March 7, 2007 lec 5W.20



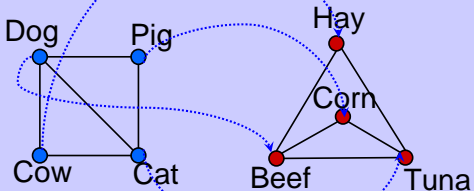
Edges Preserved? YES!




Copyright © Albert R. Meyer, 2007. All rights reserved. March 7, 2007 lec 5W.21



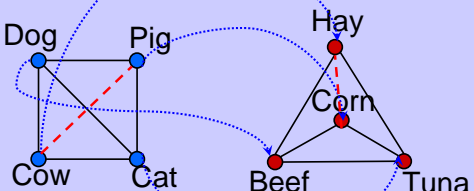
NonEdges Preserved?




Copyright © Albert R. Meyer, 2007. All rights reserved. March 7, 2007 lec 5W.22



NonEdges Preserved? YES!



Copyright © Albert R. Meyer, 2007. All rights reserved. March 7, 2007 lec 5W.23



Graph Isomorphism

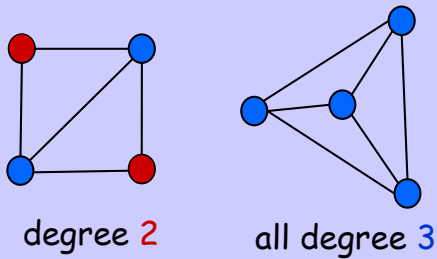
G_1 *isomorphic* to G_2 means
 there is an *edge-preserving vertex matching*.

\exists bijection $f: V_1 \rightarrow V_2$
 $u - v$ in E_1 iff $f(u) - f(v)$ in E_2

Copyright © Albert R. Meyer, 2007. All rights reserved. March 7, 2007 lec 5W.24

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

Non-isomorphism



Copyright © Albert R. Meyer, 2007. All rights reserved.

March 7, 2007

lec 5W.25

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

Finding the Mapping?

Not easy --many possible mappings.

Can test for *properties preserved under isomorphism*:

of nodes, # edges,
degree distributions,
length of paths & cycles ...

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 7, 2007

lec 5W.26

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

Connectedness

Copyright © Albert R. Meyer, 2007. All rights reserved.

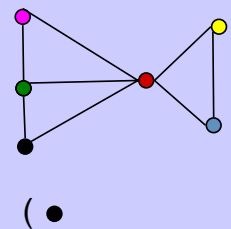
March 7, 2007

lec 5W.27

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

Paths

Path: sequence of *adjacent* vertices



Copyright © Albert R. Meyer, 2007. All rights reserved.

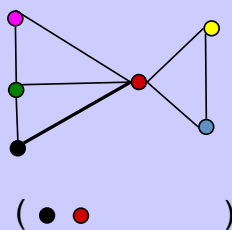
March 7, 2007

lec 5W.28

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

Paths

Path: sequence of *adjacent* vertices



Copyright © Albert R. Meyer, 2007. All rights reserved.

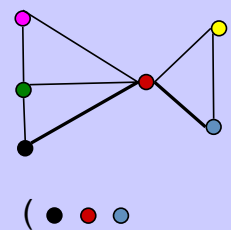
March 7, 2007

lec 5W.29

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

Paths

Path: sequence of *adjacent* vertices



Copyright © Albert R. Meyer, 2007. All rights reserved.

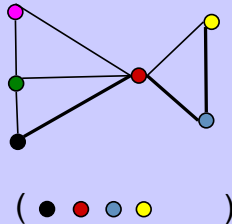
March 7, 2007

lec 5W.30

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

Paths

Path: sequence of *adjacent* vertices



Copyright © Albert R. Meyer, 2007. All rights reserved.

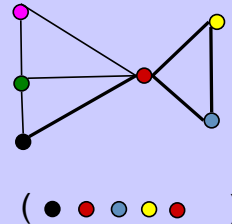
March 7, 2007

lec 5W.31

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

Paths

Path: sequence of *adjacent* vertices



Copyright © Albert R. Meyer, 2007. All rights reserved.

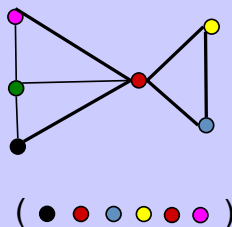
March 7, 2007

lec 5W.32

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

Paths

Path: sequence of *adjacent* vertices



Copyright © Albert R. Meyer, 2007. All rights reserved.

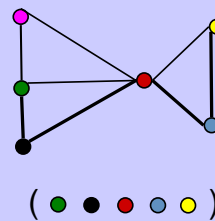
March 7, 2007

lec 5W.33

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

Simple Paths

Simple Path: all vertices different



Copyright © Albert R. Meyer, 2007. All rights reserved.

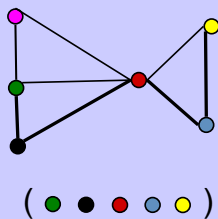
March 7, 2007

lec 5W.34

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

Simple Paths

Simple Path: (doesn't cross itself)



Copyright © Albert R. Meyer, 2007. All rights reserved.

March 7, 2007

lec 5W.35

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

Connectedness

vertices v , w are *connected* iff there is a path starting at v and ending at w .

A graph is *connected* iff every pair of vertices are connected.

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 7, 2007

lec 5W.36



1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Team Problems

Problems

2,3,1,4

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 7, 2007

lec 5W.37

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

Simple Graphs: Connectedness, Trees

Copyright © Albert R. Meyer, 2007. All rights reserved. March 9, 2007

lec 5F.1

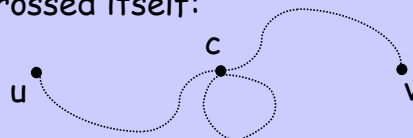
6	9	13	7
12		10	5
3	1	4	14
15	8	11	2

Paths & Simple Paths

Lemma:

The *shortest* path between two vertices is *simple*!

Proof: Suppose path from u to v crossed itself:



Copyright © Albert R. Meyer, 2007. All rights reserved. March 9, 2007

lec 5F.2

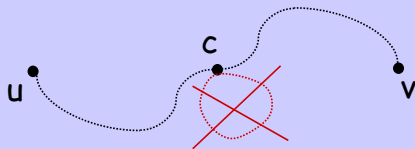
6	9	13	7
12		10	5
3	1	4	14
15	8	11	2

Paths & Simple Paths

Lemma:

The *shortest* path between two vertices is *simple*!

Then path without $c \cdots c$ is shorter:



Copyright © Albert R. Meyer, 2007. All rights reserved. March 9, 2007

lec 5F.3

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

Connected Graphs

A *connected* graph:
there is a path between
every two vertices.

Copyright © Albert R. Meyer, 2007. All rights reserved. March 9, 2007

lec 5F.4

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

Connected Components

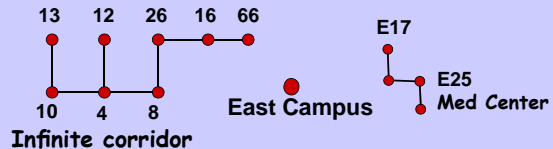
Every graph consists of
separate connected
pieces (subgraphs) called
connected components

Copyright © Albert R. Meyer, 2007. All rights reserved. March 9, 2007

lec 5F.5

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

Connected Components



Infinite corridor

3 connected components

The more connected components,
the more "broken up" the graph is.

Copyright © Albert R. Meyer, 2007. All rights reserved. March 9, 2007

lec 5F.6

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Connected Components

The *connected component* of vertex v :

$$\{w \mid v \text{ and } w \text{ are connected}\}$$

Copyright © Albert R. Meyer, 2007. All rights reserved. March 9, 2007

lec 5F.7

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Connected Components

So a graph is **connected** iff it has only **1 connected component**

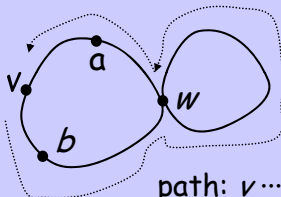
Copyright © Albert R. Meyer, 2007. All rights reserved. March 9, 2007

lec 5F.8

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Cycles

A **cycle** is a path that begins and ends with same vertex



path: $v \cdots b \cdots w \cdots a \cdots v$

also: $a \cdots v \cdots b \cdots w \cdots a$

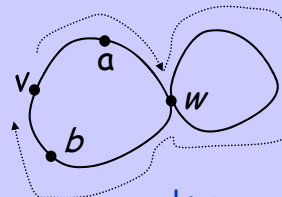
Copyright © Albert R. Meyer, 2007. All rights reserved. March 9, 2007

lec 5F.9

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Cycles

A **cycle** is a path that begins and ends with same vertex



also: $a \cdots w \cdots b \cdots v \cdots a$

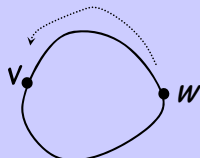
Copyright © Albert R. Meyer, 2007. All rights reserved. March 9, 2007

lec 5F.10

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Simple Cycles

A simple **cycle** is a cycle that doesn't cross itself



path: $v \cdots w \cdots v$ also: $w \cdots v \cdots w$

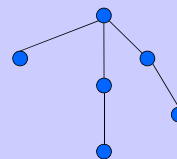
Copyright © Albert R. Meyer, 2007. All rights reserved. March 9, 2007

lec 5F.11

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Trees

A **tree** is a connected graph with no cycles.

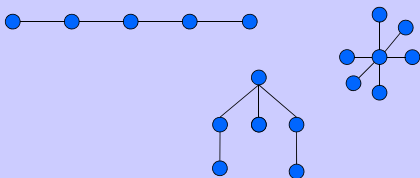


Copyright © Albert R. Meyer, 2007. All rights reserved. March 9, 2007

lec 5F.12

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

More Trees



Copyright © Albert R. Meyer, 2007. All rights reserved. March 9, 2007

lec 5F.13

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Other Tree Definitions

- A tree is a graph with a *unique* path between any 2 vertices.
- A tree is a connected graph with n vertices and $n - 1$ edges.
- A tree is an *edge-minimal* connected graph.

Copyright © Albert R. Meyer, 2007. All rights reserved. March 9, 2007

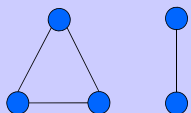
lec 5F.14

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Be careful with these definitions

Is a tree simply a graph with n vertices and $n - 1$ edges?

NO:

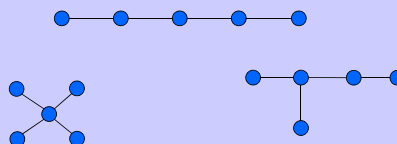


Copyright © Albert R. Meyer, 2007. All rights reserved. March 9, 2007

lec 5F.15

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Some trees with five vertices

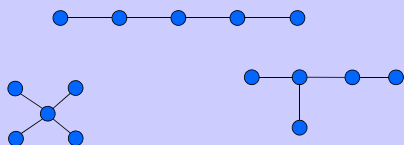


Copyright © Albert R. Meyer, 2007. All rights reserved. March 9, 2007

lec 5F.16

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Some trees with five vertices



Exercise: Prove that all trees with five vertices are isomorphic to one of these three.

Copyright © Albert R. Meyer, 2007. All rights reserved. March 9, 2007

lec 5F.17

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Spanning Trees

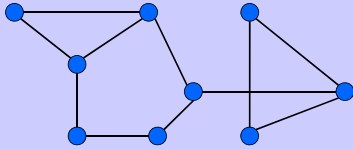
A *spanning tree*: a subgraph that is a tree on all the vertices.

Copyright © Albert R. Meyer, 2007. All rights reserved. March 9, 2007

lec 5F.19

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

Spanning Trees

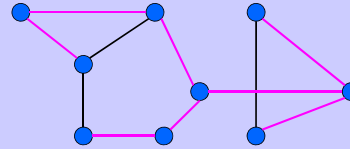


Copyright © Albert R. Meyer, 2007. All rights reserved. March 9, 2007

lec 5F.20

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

Spanning Trees



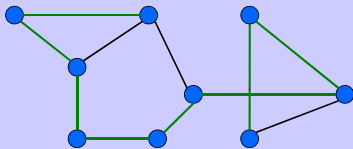
a spanning tree

Copyright © Albert R. Meyer, 2007. All rights reserved. March 9, 2007

lec 5F.21

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

Spanning Trees



another spanning tree
(can have many)

Copyright © Albert R. Meyer, 2007. All rights reserved. March 9, 2007

lec 5F.22

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

Spanning Trees

A *spanning tree*: a subgraph that is a tree on all the vertices.

Always exists: find *minimum edge-size*, connected subgraph on all the vertices.

Copyright © Albert R. Meyer, 2007. All rights reserved. March 9, 2007

lec 5F.23

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

CONNECTEDNESS

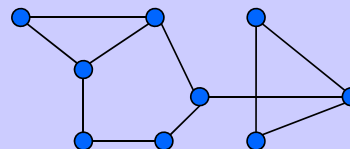
An edge is a *cut edge* if removing it from the graph *disconnects* two vertices.

Copyright © Albert R. Meyer, 2007. All rights reserved. March 9, 2007

lec 5F.24

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

Cut Edges

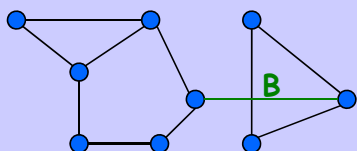


Copyright © Albert R. Meyer, 2007. All rights reserved. March 9, 2007

lec 5F.25

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

Cut Edges



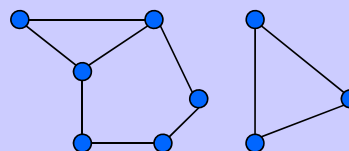
B is a cut edge

Copyright © Albert R. Meyer, 2007. All rights reserved. March 9, 2007

lec 5F.26

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

Cut Edges



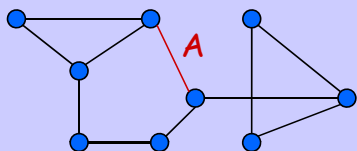
deleting **B** gives
two components

Copyright © Albert R. Meyer, 2007. All rights reserved. March 9, 2007

lec 5F.27

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

Cut Edges



A is *not* a cut edge

Copyright © Albert R. Meyer, 2007. All rights reserved. March 9, 2007

lec 5F.28

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

Cut Edges and Cycles

Lemma: An edge is a cut edge iff it is not traversed by a simple cycle.

Proof: problem set

Copyright © Albert R. Meyer, 2007. All rights reserved. March 9, 2007

lec 5F.29

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

Cut Edges

Fault-tolerant design:

In a tree, every edge is a cut edge (bad)

In a mesh, no edge is a cut edge (good; 2-connected)

Tradeoff edges for failure tolerance

Copyright © Albert R. Meyer, 2007. All rights reserved. March 9, 2007

lec 5F.30

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

k-Connectedness

*Def: **k**-connected iff need to delete **k** edges to disconnect.*

Copyright © Albert R. Meyer, 2007. All rights reserved. March 9, 2007

lec 5F.31

4	9	13	7
12		10	6
3	1	14	15
16	8	11	5

k-Connectedness

Def: k -connected iff
remains connected
when any $k-1$ edges
are deleted.

Copyright © Albert R. Meyer, 2007. All rights reserved. March 9, 2007

lec 5F.32

4	9	13	7
12		10	6
3	1	14	15
16	8	11	5

k-Connectedness

Example:

K_n is $(n-1)$ -connected

Copyright © Albert R. Meyer, 2007. All rights reserved. March 9, 2007

lec 5F.33

4	9	13	7
12		10	6
3	1	14	15
16	8	11	5

Team Problems

Problems
1–3

Copyright © Albert R. Meyer, 2007. All rights reserved. March 9, 2007

lec 5F.34



Graph Coloring

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 12, 2007

lec 6M.1



Flight Gates



flights need gates, but
times overlap.
how many gates needed?

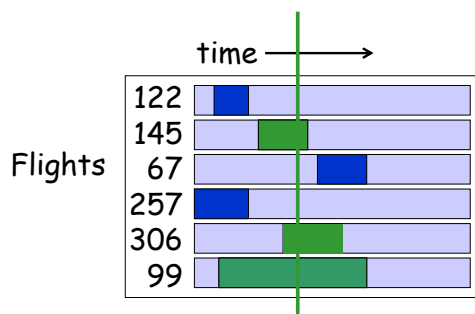
Copyright © Albert R. Meyer, 2007. All rights reserved.

March 12, 2007

lec 6M.2



Airline Schedule



Copyright © Albert R. Meyer, 2007. All rights reserved.

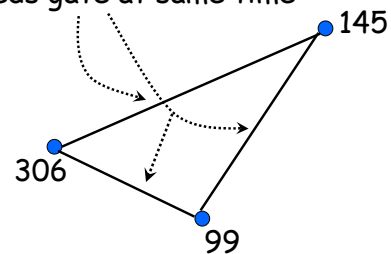
March 12, 2007

lec 6M.3



Conflicts Among Three

Needs gate at same time



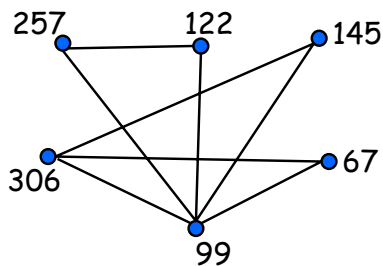
Copyright © Albert R. Meyer, 2007. All rights reserved.

March 12, 2007

lec 6M.4



Model all Conflicts with a Graph



Copyright © Albert R. Meyer, 2007. All rights reserved.

March 12, 2007

lec 6M.5



Color vertices



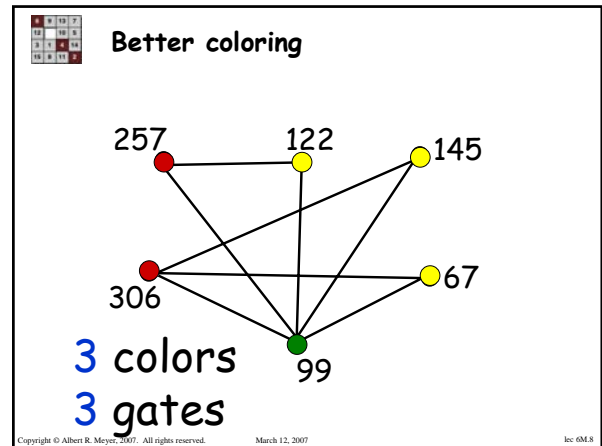
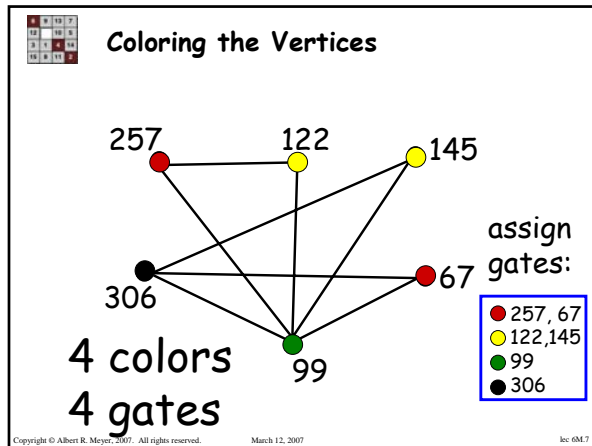
so adjacent vertices have
different colors.

colors = # gates needed

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 12, 2007

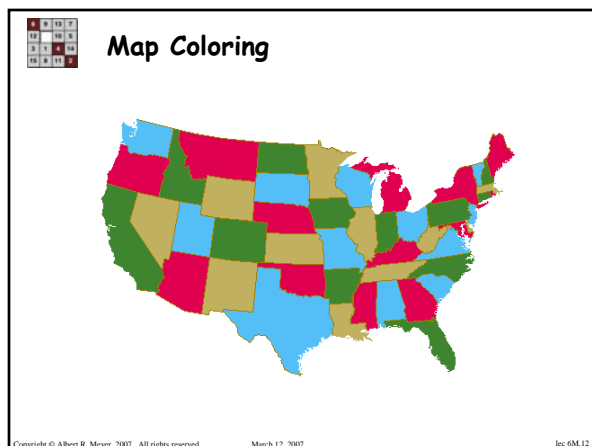
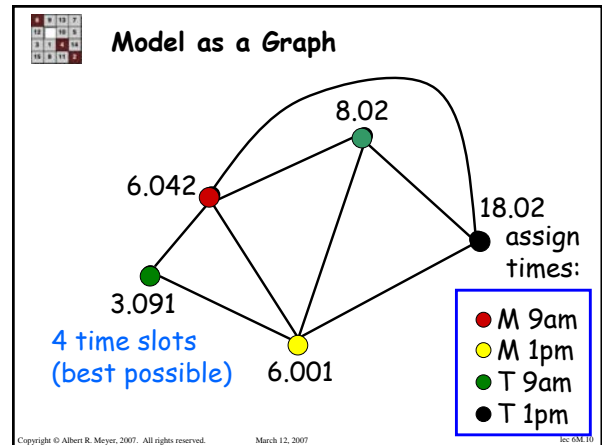
lec 6M.6



Final Exams

subjects **conflict** if student
takes both, so
need different time slots.
how short an exam period?

Copyright © Albert R. Meyer, 2007. All rights reserved. March 12, 2007 lec 6M.9



Four Color Theorem

any **planar map** is **4-colorable**.
 1850's: false proof published
 (was correct for 5 colors).
 1970's: prf with much computing
 1990's: much improved

Copyright © Albert R. Meyer, 2007. All rights reserved. March 12, 2007 lec 6M.14

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

Chromatic Number

min #colors for G is
chromatic number, $\chi(G)$

lemma:

$$\chi(\text{tree}) = 2$$

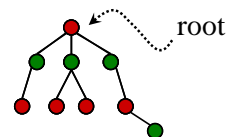
Copyright © Albert R. Meyer, 2007. All rights reserved.

March 12, 2007

lec 6M.15

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

Trees are 2-colorable



Pick any vertex as "root."
if (unique) path from root is
even length: ●
odd length: ●

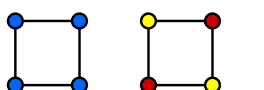
Copyright © Albert R. Meyer, 2007. All rights reserved.

March 12, 2007

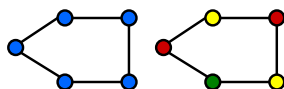
lec 6M.16

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

Simple Cycles



$$\chi(C_{\text{even}}) = 2$$



$$\chi(C_{\text{odd}}) = 3$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 12, 2007

lec 6M.17

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

Complete Graph K_5



$$\chi(K_n) = n$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 12, 2007

lec 6M.18

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

Bounded Degree

if all vertex degrees $\leq k$, then

$$\chi(G) \leq k+1$$

... by simple recursive
coloring procedure

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 12, 2007

lec 6M.20

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

Coloring with d_{\max} colors

Induction Hypothesis $P(n) ::=$
if G has n vertices, all degrees $\leq d_{\max}$,
then $\chi(G) \leq d_{\max} + 1$ colors

Base Case: works for $n=1$ vertex

Inductive Step: given $n+1$ vertex graph

- * remove one vertex
- * color remaining graph in $\leq d_{\max} + 1$ colors
- * put vertex back. since degree $\leq d_{\max}$, must be one color left over for it.

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 12, 2007

lec 6M.21

6	9	13	7
12		10	5
3	1	14	11
15	8	16	4

Arbitrary Graphs

2-colorable? --easy to check
 3-colorable? --hard to check
 (even if planar)
 find $\chi(G)$? --theoretically
 no harder than 3-color, but
 harder in practice

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 12, 2007

lec 6M.23

6	9	13	7
12		10	5
3	1	14	11
15	8	16	4

Team Problems

Problems
 1–3

Copyright © Albert R. Meyer, 2006. All rights reserved.

March 10, 2006

lec 5F.24

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

Mathematics for Computer Science

MIT 6.042J/18.062J

Bipartite Matching

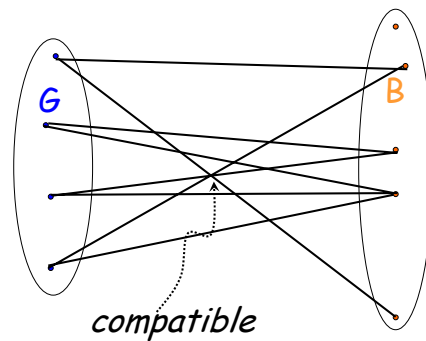
Copyright © Albert R. Meyer, 2007. All rights reserved.

March 14, 2007

lec 6W.1

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

Compatible Boys & Girls



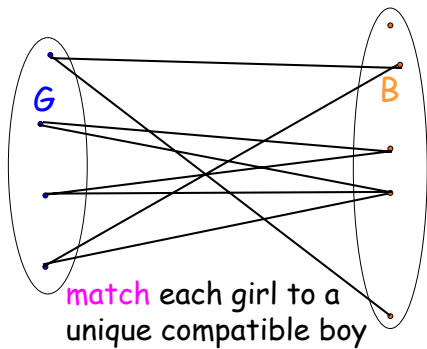
Copyright © Albert R. Meyer, 2007. All rights reserved.

March 14, 2007

lec 6W.2

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

Compatible Boys & Girls



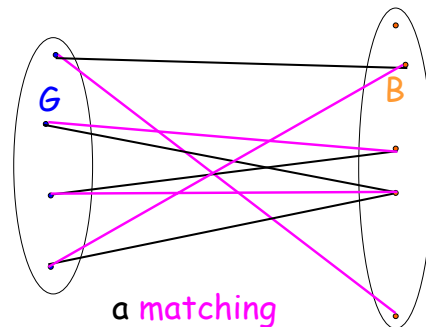
Copyright © Albert R. Meyer, 2007. All rights reserved.

March 14, 2007

lec 6W.3

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

Compatible Boys & Girls



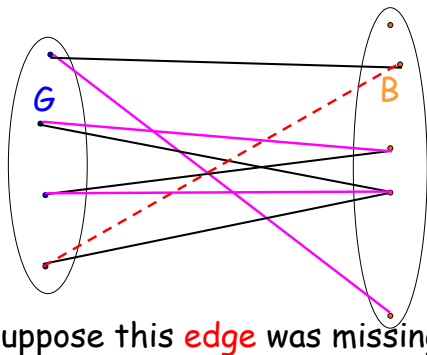
Copyright © Albert R. Meyer, 2007. All rights reserved.

March 14, 2007

lec 6W.4

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

Compatible Boys & Girls



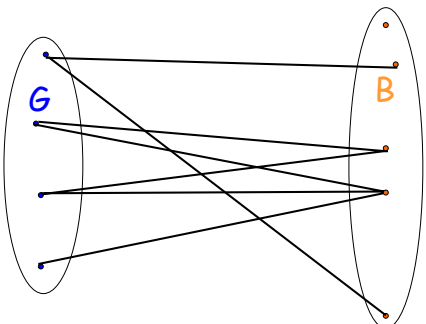
Copyright © Albert R. Meyer, 2007. All rights reserved.

March 14, 2007

lec 6W.5

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

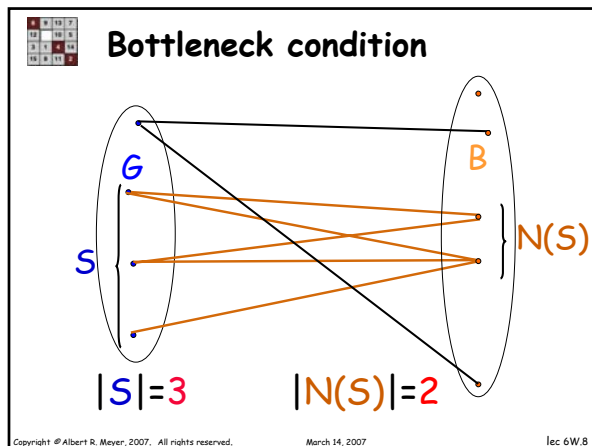
No match possible



Copyright © Albert R. Meyer, 2007. All rights reserved.

March 14, 2007

lec 6W.6



Bottleneck Lemma

bottleneck: not enough boys for some set of girls.

$N(S) ::= \{b \mid b \text{ adjacent to an } s \in S\},$
 $|S| > |N(S)|$

If there is a bottleneck,
 then no match is possible.

Copyright © Albert R. Meyer, 2007. All rights reserved. March 14, 2007 lec 6W.9

Hall's Theorem

Conversely, if there are
 no bottlenecks, then
 there is a perfect match

Copyright © Albert R. Meyer, 2007. All rights reserved. March 14, 2007 lec 6W.10

Hall's Theorem

Assume no bottlenecks.

Lemma: If S is a set of girls and
 $|S| = |N(S)|,$
 then there are no
 bottlenecks within S
 (obviously)

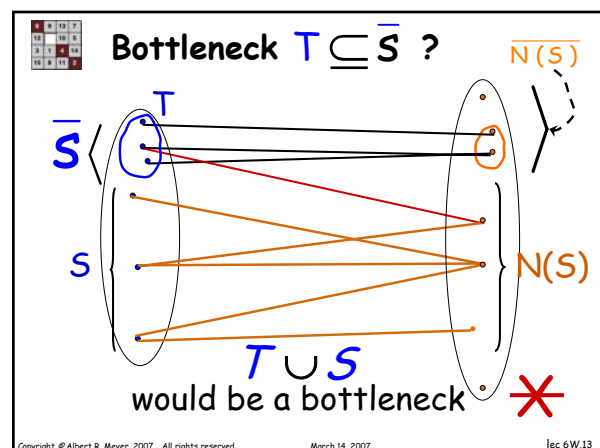
Copyright © Albert R. Meyer, 2007. All rights reserved. March 14, 2007 lec 6W.11

Hall's Theorem

Assume no bottlenecks.

Lemma: If S is a set of girls and
 $|S| = |N(S)|,$
 and no bottlenecks
 between \bar{S} and $N(S)$

Copyright © Albert R. Meyer, 2007. All rights reserved. March 14, 2007 lec 6W.12



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

Hall's Theorem

no bottlenecks implies
perfect match

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 14, 2007

lec 6W.14

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

Hall's Theorem

proof by induction on # girls.
case: proper subset, S ,
of girls with

$$|S| = |N(S)|$$

By Lemma no bottlenecks in
bipartite graph $(S, N(S))$,
and none in $(\overline{S}, \overline{N(S)})$

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 14, 2007

lec 6W.15

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

Hall's Theorem

by induction match
 $(S, N(S))$, and
 $(\overline{S}, \overline{N(S)})$
separately.

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 14, 2007

lec 6W.16

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

Hall's Theorem

case: $|S| < |N(S)|$ always.
match 1st girl with a boy.
remaining girls & boys won't
have any bottlenecks, so
by induction can match them

QED

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 14, 2007

lec 6W.17

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

How to verify no bottlenecks?

Every girl likes $\geq d$ boys, and
every boy likes $\leq d$ girls,
implies no bottlenecks.

proof: any set S of girls with e
incident edges:

$$d|S| \leq e \leq d|N(S)|$$

$$|S| \leq |N(S)|$$

(no bottleneck)

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 14, 2007

lec 6W.18

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

Team Problem

Problems
1–3

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 14, 2007

lec 6W.19

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

Mathematics for Computer Science
MIT 6.042J/18.062J

Directed Graphs; Communication Networks

Copyright © Albert R. Meyer, 2007. All rights reserved. March 16, 2007

lec 6F.1

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

Digraphs

a set, V , of *vertices*

a set, $E \subseteq V \times V$

of *directed edges*.

$(v, w) \in E$ notation: $v \rightarrow w$



Copyright © Albert R. Meyer, 2007. All rights reserved. March 16, 2007

lec 6F.2

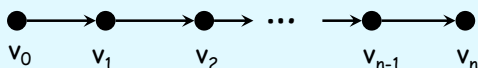
6	9	13	7
12		10	5
3	1	4	14
15	8	11	2

Digraphs

paths are directed:

v_0, v_1, \dots, v_n

where $v_i \rightarrow v_{i+1}$ for all i



Copyright © Albert R. Meyer, 2007. All rights reserved. March 16, 2007

lec 6F.3

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

Path Relation: Connectedness

v is *connected to* w :

there is a path

$v \rightarrow \dots \rightarrow w$

(length 0 path from v to v)

Copyright © Albert R. Meyer, 2007. All rights reserved. March 16, 2007

lec 6F.4

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

Positive Path Relation

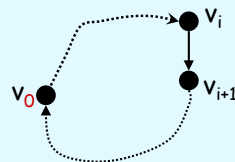
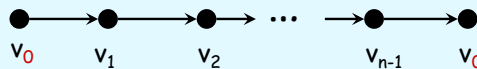
v is *connected to* w by a
positive length path

Copyright © Albert R. Meyer, 2007. All rights reserved. March 16, 2007

lec 6F.5

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

Directed Cycles



Copyright © Albert R. Meyer, 2007. All rights reserved. March 16, 2007

lec 6F.6

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

Digraphs

Formally, a Digraph, D , is *exactly the same* as a binary relation on the vertices.

irreflexive:



asymmetric:



Copyright © Albert R. Meyer, 2007. All rights reserved. March 16, 2007

lec 6F.7

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

Directed Acyclic Graph's

DAG's represent **strict partial orders**:

- The positive path relation of a DAG is a strict p.o.
- Every partial order is the positive path relation of a DAG.

Copyright © Albert R. Meyer, 2007. All rights reserved. March 16, 2007

lec 6F.8

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

Communication Networks

In particular,
Permutation Networks

Copyright © Albert R. Meyer, 2007. All rights reserved. March 16, 2007

lec 6F.9

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

Permutation Networks

Digraphs with
 n designated **input vertices**
with outdegree 1



Copyright © Albert R. Meyer, 2007. All rights reserved. March 16, 2007

lec 6F.10

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

Permutation Networks

and with
 n designated **output vertices**
with indegree 1



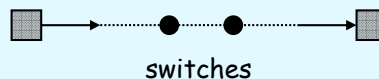
Copyright © Albert R. Meyer, 2007. All rights reserved. March 16, 2007

lec 6F.11

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

Permutation Networks

and for *every* input and
output, there is a path



Copyright © Albert R. Meyer, 2007. All rights reserved. March 16, 2007

lec 6F.12

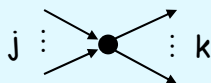
6	9	13	7
12		10	5
3	1	4	14
15	8	11	2

Network Measures

diameter: largest input-output distance

size: # switches, # edges

switch degrees: $j \times k$



Copyright © Albert R. Meyer, 2007. All rights reserved. March 16, 2007

lec 6F.13

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

Permutation Routing Problems

A **routing problem** is a bijection,
 $\pi: \{1, \dots, n\} \rightarrow \{1, \dots, n\}$
 (called a *permutation*)

Copyright © Albert R. Meyer, 2007. All rights reserved. March 16, 2007

lec 6F.14

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

Permutation Routing Problems

A **solution** to a routing problem is a set of n paths from input k to input $\pi(k)$ for $k=1, \dots, n$.

Copyright © Albert R. Meyer, 2007. All rights reserved. March 16, 2007

lec 6F.15

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

Permutation Problem Solutions

Solutions commonly select *shortest paths* between input k and output $\pi(k)$.
 (but sometimes shortest paths are not best)

Copyright © Albert R. Meyer, 2007. All rights reserved. March 16, 2007

lec 6F.16

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

Permutation Problem Solutions

Quality of a *solution*:

latency: max path length

congestion: max #paths through one switch

(also *average* latency, congestion)

Copyright © Albert R. Meyer, 2007. All rights reserved. March 16, 2007

lec 6F.17

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

Difficulty of a Problem, π

Problem difficulty measured by *best* solution it allows:

problem-latency: *smallest* latency of any solution

problem-congestion: *smallest* congestion of any solution

Copyright © Albert R. Meyer, 2007. All rights reserved. March 16, 2007

lec 6F.18

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

Quality of A Network

Network quality measured by its *hardest* problem:

max-latency: *largest* problem-latency

max-congestion: *largest* problem-congestion

Copyright © Albert R. Meyer, 2007. All rights reserved. March 16, 2007

lec 6F.19

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

Quality of A Network

Finding max-congestion can be tricky. To prove $\text{max-con} \leq k$: show how, given **any** problem, π , to route packets for π with **congestion** $\leq k$.

Copyright © Albert R. Meyer, 2007. All rights reserved. March 16, 2007

lec 6F.20

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

Quality of A Network

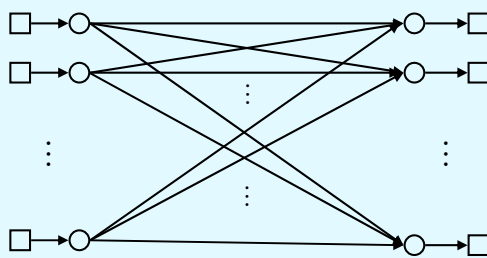
Finding max-congestion can be tricky. To prove $\text{max-con} \geq k$: must find problem, π , and show that **every** routing for π has congestion $\geq k$.

Copyright © Albert R. Meyer, 2007. All rights reserved. March 16, 2007

lec 6F.21

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

A Good, Unreasonable Network



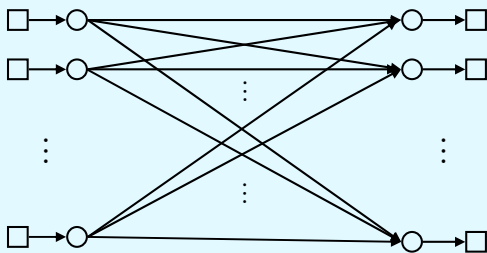
unique paths from in to out

Copyright © Albert R. Meyer, 2007. All rights reserved. March 16, 2007

lec 6F.22

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

A Good, Unreasonable Network



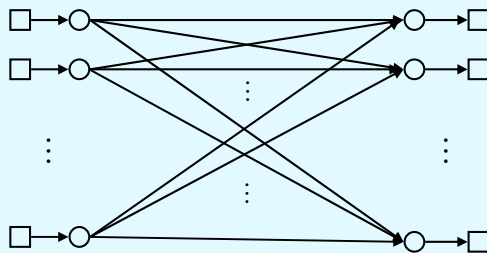
diameter = latency = 3

Copyright © Albert R. Meyer, 2007. All rights reserved. March 16, 2007

lec 6F.23

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

A Good, Unreasonable Network



max-congestion = 1

Copyright © Albert R. Meyer, 2007. All rights reserved. March 16, 2007

lec 6F.24

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

A Good, Unreasonable Network

switches = $2n$

Copyright © Albert R. Meyer, 2007. All rights reserved. March 16, 2007 lec 6F:25

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

A Good, Unreasonable Network

switch-degree: $1 \times n, n \times 1$

Copyright © Albert R. Meyer, 2007. All rights reserved. March 16, 2007 lec 6F:26

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

A Good, Unreasonable Network

#edges: $n(n+2)$

Copyright © Albert R. Meyer, 2007. All rights reserved. March 16, 2007 lec 6F:27

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

A Good, Unreasonable Network

Can be modified to use
bounded switches
(Class Problem 2).
Good in all ways
but $\approx n^2$ switches

Copyright © Albert R. Meyer, 2007. All rights reserved. March 16, 2007 lec 6F:28

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

Benés Network

Copyright © Albert R. Meyer, 2007. All rights reserved. March 16, 2007 lec 6F:29

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

A Great Network

Benés Network, B_n
handles
 $N ::= 2^n$
inputs and outputs

Copyright © Albert R. Meyer, 2007. All rights reserved. March 16, 2007 lec 6F:30

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

Benés Network

Benés Net is **small**:

latency $\approx 2 \log N$

#switches $\approx N \log N$

switch sizes = $1 \times 2, 2 \times 1$

and **max-congestion** = 1

Copyright © Albert R. Meyer, 2007. All rights reserved. March 16, 2007

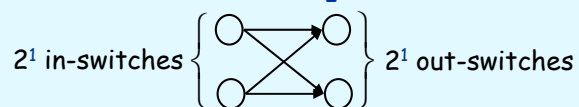
lec 6F.31

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

Benés Network

Recursive Data Type

Base case: B_1



$N = 2$

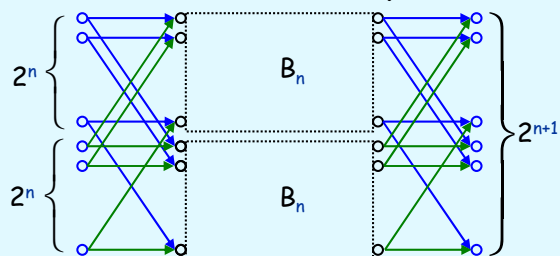
Copyright © Albert R. Meyer, 2007. All rights reserved. March 16, 2007

lec 6F.32

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

Benés Network

Constructor step: B_{n+1}



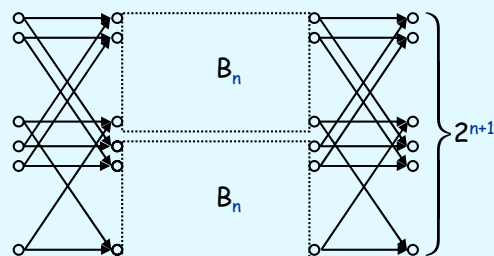
Copyright © Albert R. Meyer, 2007. All rights reserved. March 16, 2007

lec 6F.33

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

Benés Network

diam B_{n+1}



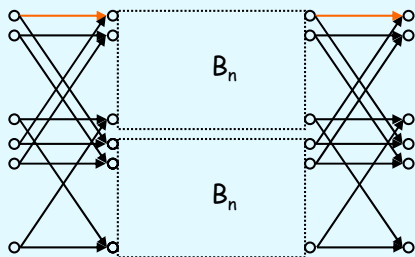
Copyright © Albert R. Meyer, 2007. All rights reserved. March 16, 2007

lec 6F.34

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

Benés Network

diam $B_{n+1} = 2 + \text{diam } B_n$



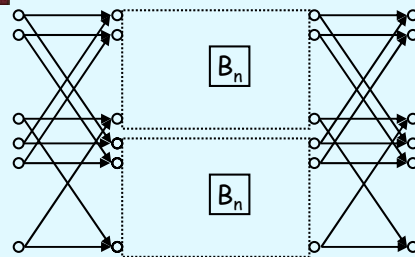
Copyright © Albert R. Meyer, 2007. All rights reserved. March 16, 2007

lec 6F.35

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

Benés Network

size $B_{n+1} =$



Copyright © Albert R. Meyer, 2007. All rights reserved. March 16, 2007

lec 6F.36

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

Benés Network

size $B_{n+1} = 2 \text{ size } B_n + 2 \cdot 2^{n+1}$

Copyright © Albert R. Meyer, 2007. All rights reserved. March 16, 2007 lec 6F:37

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

Benés Network

for congestion 1:

Copyright © Albert R. Meyer, 2007. All rights reserved. March 16, 2007 lec 6F:38

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

Benés Network

for congestion 1: route to **opposite halves**

Copyright © Albert R. Meyer, 2007. All rights reserved. March 16, 2007 lec 6F:39

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

Benés Network

for congestion 1: route to **opposite halves**

Copyright © Albert R. Meyer, 2007. All rights reserved. March 16, 2007 lec 6F:40

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

Benés Solution to π

Find 2-coloring for

$1 \text{ --- } 1+2^n$

$2 \text{ --- } 2+2^n$

\vdots

$2^n \text{ --- } 2^n+2^n$

$\pi^{-1}(1) \text{ --- } \pi^{-1}(1+2^n)$

$\pi^{-1}(2) \text{ --- } \pi^{-1}(2+2^n)$

\vdots

Copyright © Albert R. Meyer, 2007. All rights reserved. March 16, 2007 lec 6F:41

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

Team Problems

Problems 1-3

Copyright © Albert R. Meyer, 2007. All rights reserved. March 16, 2007 lec 6F:42



Planar Graphs

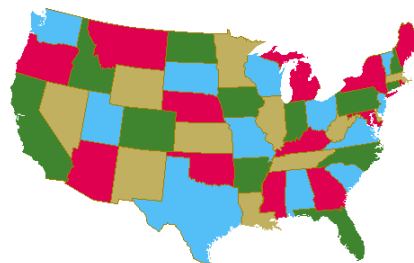
Copyright © Albert R. Meyer, 2007. All rights reserved.

March 19, 2007

lec 7m.1



Planar Graphs



Copyright © Albert R. Meyer, 2007. All rights reserved.

March 19, 2007

lec 7m.2



Planar Graphs

A graph is *planar* if there is a way to **draw** it in the plane without edges crossing.

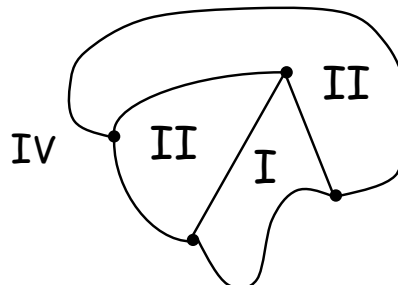
Copyright © Albert R. Meyer, 2007. All rights reserved.

March 19, 2007

lec 7m.3



Four Continuous Faces



4 Connected Regions

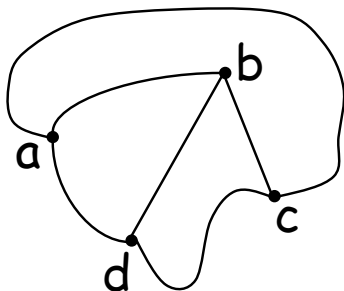
Copyright © Albert R. Meyer, 2007. All rights reserved.

March 19, 2007

lec 7m.4



Region Boundaries



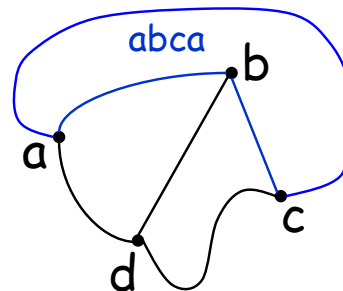
Copyright © Albert R. Meyer, 2007. All rights reserved.

March 19, 2007

lec 7m.5



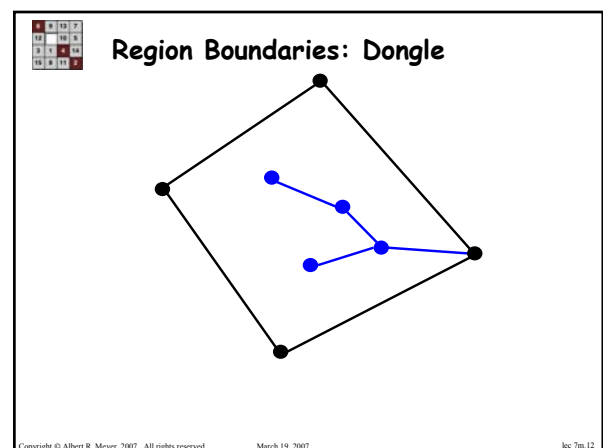
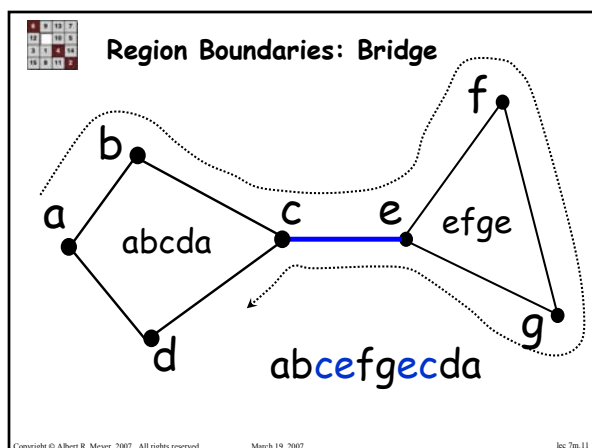
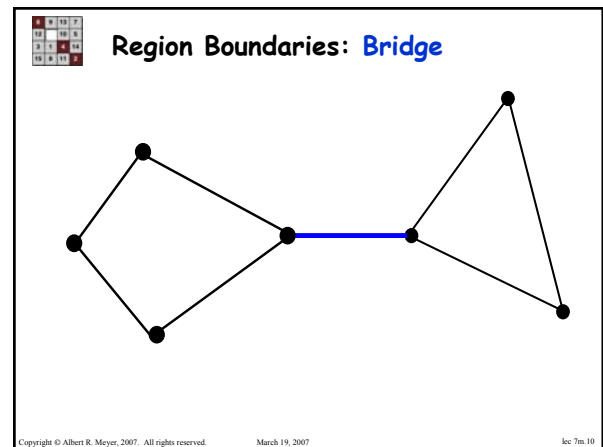
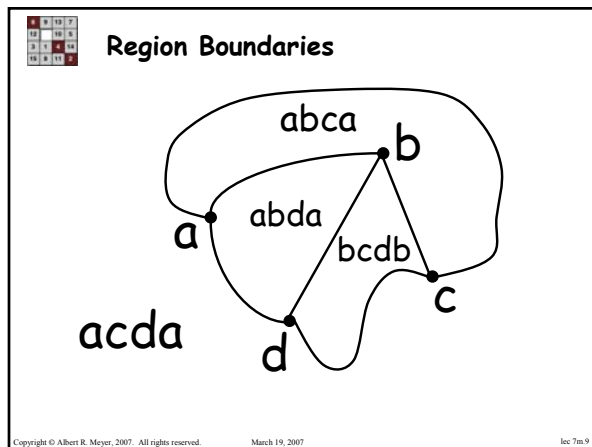
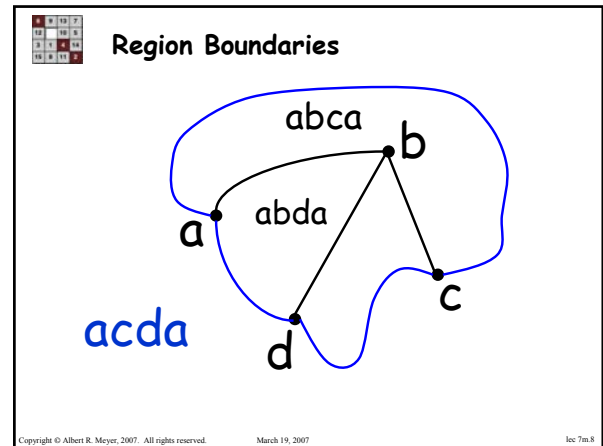
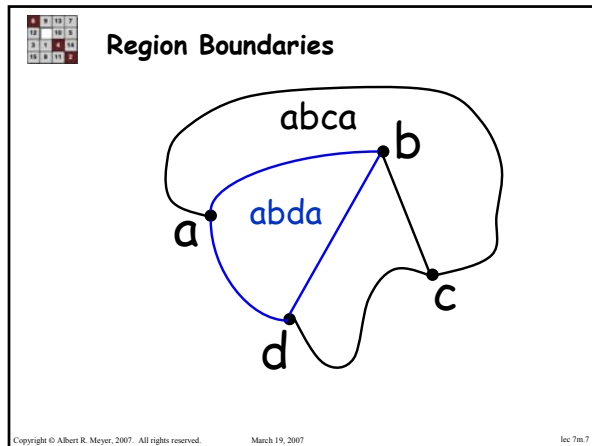
Region Boundaries

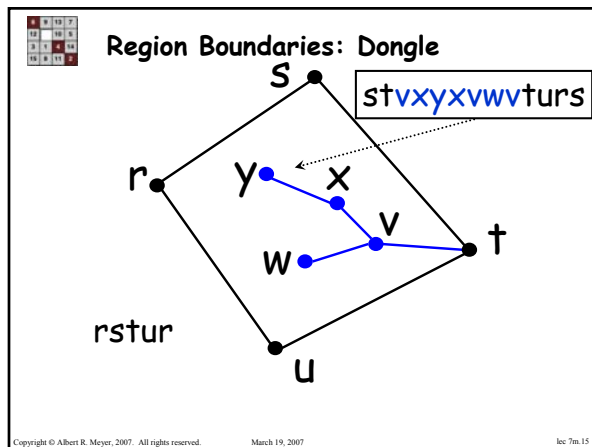
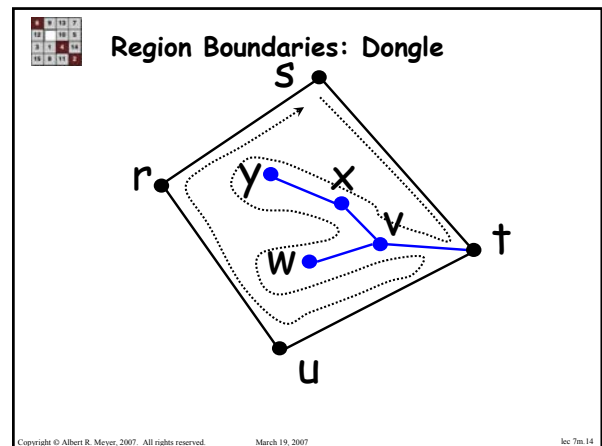
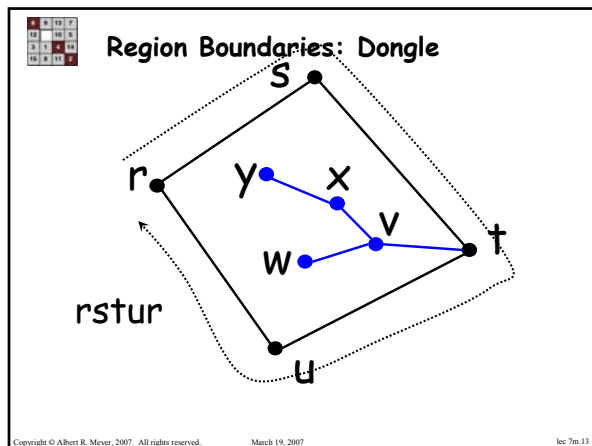


Copyright © Albert R. Meyer, 2007. All rights reserved.

March 19, 2007

lec 7m.6

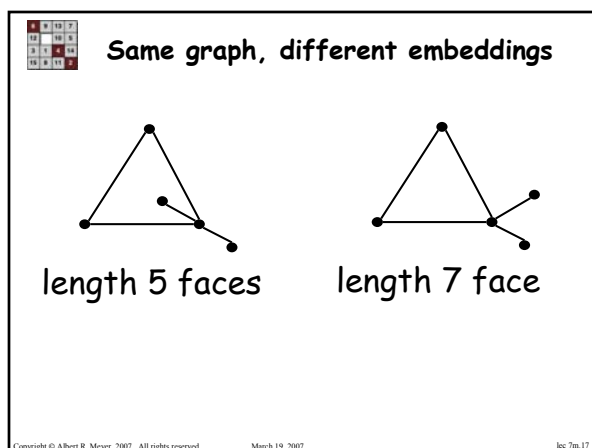




Planar Embedding

A **planar embedding** is a graph *along with* its face boundaries: cycles
(same graph may have different embeddings)

Copyright © Albert R. Meyer, 2007. All rights reserved. March 19, 2007 lec 7m.16



Recursive Def: Planar Embeddings

Base: a graph consisting of a single vertex, v , along with face: length 0 cycle from v to v , is a **PE**.

v ● ●
graph faces

Copyright © Albert R. Meyer, 2007. All rights reserved. March 19, 2007 lec 7m.18



Adding an edge to an embedding

Two constructor cases:

- 1) Add edge across a face (splits face in two)
- 2) Add bridge between components (merges 2 outer faces)

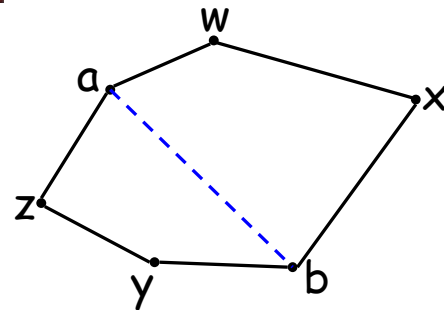
Copyright © Albert R. Meyer, 2007. All rights reserved.

March 19, 2007

lec 7m.19



Constructor: Split a Face



$awxbyza \rightarrow awxba, abyza$

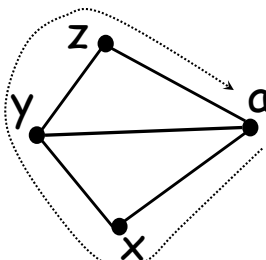
Copyright © Albert R. Meyer, 2007. All rights reserved.

March 19, 2007

lec 7m.20



Constructor: Add a Bridge



$axyza$

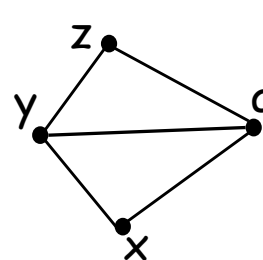
Copyright © Albert R. Meyer, 2007. All rights reserved.

March 19, 2007

lec 7m.21



Constructor: Add a Bridge



$axyza$

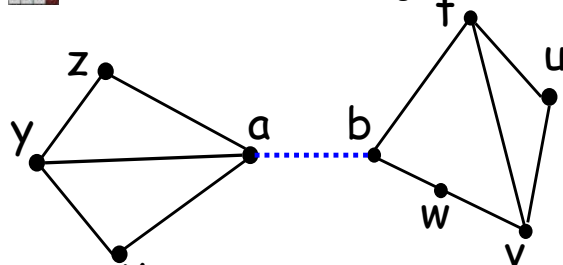
Copyright © Albert R. Meyer, 2007. All rights reserved.

March 19, 2007

lec 7m.22



Constructor: Add a Bridge



$axyza, btuvwb \rightarrow axyzabtuwvba$

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 19, 2007

lec 7m.23



Euler's Formula

If a planar embedding has v vertices, e edges, and f faces, then

$$v - e + f = 2$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 19, 2007

lec 7m.24

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

Euler's Formula

- Proof by structural induction on embeddings:
- **base case:** 1 vertex

$$v = 1, f = 1, e = 0$$

$$1 - 0 + 1 = 2$$



Copyright © Albert R. Meyer, 2007. All rights reserved.

March 19, 2007

lec 7m.25

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

Adding an edge to a drawing

Constructor case (split face):

- v stays the same
 - e increases by 1
 - f increases by 1
- so $v - e + f$ stays the same



Copyright © Albert R. Meyer, 2007. All rights reserved.

March 19, 2007

lec 7m.26

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

Adding an edge to a drawing

Constructor case (add bridge):

- $v = v_1 + v_2$
 - $e = e_1 + e_2 + 1$
 - $f = f_1 + f_2 - 1$
- $$(v_1 + v_2) - (e_1 + e_2 + 1) + (f_1 + f_2 - 1)$$
- $$= 2 + 2 - 2 = 2$$



Copyright © Albert R. Meyer, 2007. All rights reserved.

March 19, 2007

lec 7m.27

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

Euler's Formula

Corollary:

There are at most
5 regular polyhedra

(proof in Notes)

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 19, 2007

lec 7m.28

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

Planar Properties

- each edge appears twice on faces
- face length ≥ 3 (for $v \geq 3$)

$$\text{so } 3f \leq 2e$$

combining with Euler:

$$e \leq 3v - 6$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 19, 2007

lec 7m.29

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

Planar Properties

- each edge appears twice on faces
 - face length ≥ 3 (for $v \geq 3$)
 - can draw edges in any order
- (proofs by structural induction)

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 19, 2007

lec 7m.30

6	9	13	7
12		10	5
3	1	14	11
15	8	16	4

Planar Properties: Corollaries

- K_5 and $K_{3,3}$ not planar
- \exists vertex of degree ≤ 5
- subgraphs are planar
- 6-colorable

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 19, 2007

lec 7m.31

6	9	13	7
12		10	5
3	1	14	11
15	8	16	4

Team Problems

Problems 1–3

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 19, 2007

lec 7m.32

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

Mathematics for Computer Science

MIT 6.042J/18.062J

Intro to Number Theory: Divisibility, GCD's

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.1

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

Arithmetic Assumptions

Algebraic rules for $+$, $-$, \times :

$$a(b+c) = ab + ac, \quad ab = ba,$$

$$(ab)c = a(bc), \quad a - a = 0,$$

$$a + 0 = a, \quad a+1 > a, \dots$$

We take these for granted!

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.2

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

Divisibility

a "divides" b ($a|b$):

$$b = ak \text{ for some } k$$

$$5|15 \text{ because } 15 = 3 \cdot 5$$

$$n|0 \text{ because } 0 = n \cdot 0$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.3

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

Simple Divisibility Facts

$$a|b \text{ implies } a|bc$$

$$a|b \text{ and } b|c \text{ implies } a|c$$

$$a|b \text{ iff } ac|bc$$

$$\text{for } c \neq 0$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.4

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

Common Divisors, GCD

c is a common divisor of a and b means $c|a$ and $c|b$.

$\gcd(a,b) ::=$ the greatest common divisor of a and b .

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.5

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

GCD with a prime

If p is prime, and p does not divide a , then

$$\gcd(p,a) = 1.$$

Pf: The only divisors of p are 1 & p .

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.6

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

Divisibility of a Sum

A common divisor of two terms divides their sum.

pf: say $c|x$ and $c|y$, so

$x=k'c$, $y=k''c$. Then

$$x+y = k'c+k''c = c\underbrace{(k'+k'')}_k.$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.7

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

Divisibility of Linear Comb.

A common divisor of a & b divides any integer linear combination of a & b .

integer lin. comb.: $sa + tb$

proof: divisor of a & b divides both sa and tb .

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.8

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

The Division Theorem

For $b > 0$ and any a , there are *unique* numbers

$q ::= \text{quotient}(a,b)$,

$r ::= \text{remainder}(a,b)$, such that

$$a = qb + r \text{ and } 0 \leq r < b.$$

Take this for granted too!

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.11

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

Corollary

The remainder of a divided by b is an integer linear combination of a & b :

$$a = qb + r, \text{ so}$$

$$r = (-q) \cdot b + 1 \cdot a$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.12

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

GCD is a linear combination

Theorem: $\text{gcd}(a,b)$ is the smallest positive linear combination of a and b .

$$\text{spc}(a,b)$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.13

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

1st show: $\text{gcd}(a,b) \leq \text{spc}(a,b)$

proof: Common divisor of a, b divides lin. comb. of a & b , so

$$\text{gcd}(a,b) \mid \text{spc}(a,b).$$

In particular,

$$\text{gcd}(a,b) \leq \text{spc}(a,b).$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.14

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

2nd: $\text{spc}(a,b) \leq \text{gcd}(a,b)$

Enough to show that $\text{spc}(a,b)$ is a common divisor of *just* a .

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.15

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

Lemma: $\text{spc}(a,b) \mid a$

Pf: Remainder of a divided by $\text{spc}(a,b)$, is a linear comb. of a & b . Since remainder $<$ divisor, and divisor is smallest positive, remainder must be 0. That is, $\text{spc}(a,b)$ divides a .

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.16

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

Prime Divisibility

Lemma: p prime and $p \mid a \cdot b$ implies $p \mid a$ or $p \mid b$.

pf: say $\neg(p \mid a)$. so $\text{gcd}(p,a)=1$.

$$\begin{aligned} \text{so, } sa + tp &= 1 \\ (sa)b + (tp)b &= b \\ \underbrace{sa}_p \underbrace{b}_p + \underbrace{tp}_p \underbrace{b}_p &= b \\ p \mid p \mid \text{so } p \mid b \end{aligned}$$

QED

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.17

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

Prime Divisibility

Cor: If p is prime, and $p \mid a_1 \cdot a_2 \cdots a_m$

then $p \mid a_i$ for some i .

pf: By induction on m .

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.18

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

Finding s and t

Given a,b , how to find s,t so that $sa+tb=\text{gcd}(a,b)$?

Method: apply Euclidean algorithm, finding coefficients as you go.

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.19

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

Finding s and t

Example: $a = 899, b = 493$

$$899 = 1 \cdot 493 + 406$$

$$493 = 1 \cdot 406 + 87$$

$$406 = 4 \cdot 87 + 58$$

$$87 = 1 \cdot 58 + 29$$

$$58 = 2 \cdot 29 + 0$$

done, $\text{gcd} = 29$

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.20

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

Finding s and t

Example: $a = 899$, $b = 493$

$$\begin{aligned} 899 &= 1 \cdot 493 + 406 & \text{so } 406 &= 1 \cdot 899 + -1 \cdot 493 \\ 493 &= 1 \cdot 406 + 87 & \text{so } 87 &= 493 - 1 \cdot 406 \\ & & &= -1 \cdot 899 + 2 \cdot 493 \\ 406 &= 4 \cdot 87 + 58 & \text{so } 58 &= 406 - 4 \cdot 87 \\ & & &= 5 \cdot 899 + -9 \cdot 493 \\ 87 &= 1 \cdot 58 + 29 & \text{so } 29 &= 87 - 1 \cdot 58 \\ & & &= -6 \cdot 899 + 11 \cdot 493 \\ 58 &= 2 \cdot 29 + 0 & \text{done, gcd} &= 29 \end{aligned}$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.21

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

Finding s and t

Example: $a = 899$, $b = 493$

$$\begin{aligned} 899 &= 1 \cdot 493 + 406 & \text{so } 406 &= 1 \cdot 899 + -1 \cdot 493 \\ 493 &= 1 \cdot 406 + 87 & \text{so } 87 &= 493 - 1 \cdot 406 \\ & & &= -1 \cdot 899 + 2 \cdot 493 \\ 406 &= 4 \cdot 87 + 58 & \text{so } 58 &= 406 - 4 \cdot 87 \\ & & &= 5 \cdot 899 + -9 \cdot 493 \\ 87 &= 1 \cdot 58 + 29 & \text{so } 29 &= 87 - 1 \cdot 58 \\ & & &= -6 \cdot 899 + 11 \cdot 493 \\ 58 &= 2 \cdot 29 + 0 & \text{done, gcd} &= 29 \\ & & & \mathbf{s = -6, t = 11} \end{aligned}$$

the Pulverizer

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.22

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

Finding $s > 0$ and t

$$\begin{aligned} \text{gcd}(899, 493) &= -6 \cdot 899 + 11 \cdot 493 \\ \text{get positive coeff. for } 899? & \\ (-6 + 493k) \cdot 899 + (11 - 899k) \cdot 493 & \\ = -6 \cdot 899 + 11 \cdot 493 & \\ \text{so use } k=1: 487 \cdot 899 + -888 \cdot 493 & \\ = \text{gcd}(899, 493) & \end{aligned}$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.23

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

Generalized Die Hard

Did it with buckets:

3 gal. & 5 gal.

3 gal. & 9 gal.

Now a gal. and b gal.?

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.24

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

Generalized Die Hard

Can get *any* linear combination of a , b in a Die Hard bucket (if there's room for it).

Namely, say $0 \leq sa + tb < b$.

Get $sa + tb$ into the b gal. bucket as follows:

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.26

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

Generalized Die Hard

assume $s > 0$. do s times:

- fill bucket a , pour into b
-- if b fills, empty it.

total poured = sa

$0 \leq \text{amount left} \leq b$

times b emptied must be $-t$

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.27



1	2	3
4	5	6
7	8	9

Generalized Die Hard

- In fact, no need to count:
- fill bucket *a*, pour into *b*
-- if *b* fills, empty it.
until desired amount is in *b* !

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.28



1	2	3
4	5	6
7	8	9

Team Problems

Problems 1—3

Copyright © Albert R. Meyer, 2007. All rights reserved.

March 21, 2007

lec 7W.35

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

5-Color Theorem; Benés Network

Copyright © Albert R. Meyer, 2007. All rights reserved. March 23, 2007

lec 7F.1

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

5-Color Theorem

Planar Graphs are 5-Colorable

Copyright © Albert R. Meyer, 2007. All rights reserved. March 23, 2007

lec 7F.2

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

Planar Graphs

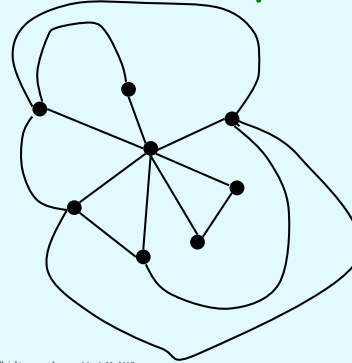
- $\deg(v) \leq 5$ for some v
- K_5 is **not** planar
- subgraphs are planar
- two new facts:

Copyright © Albert R. Meyer, 2007. All rights reserved. March 23, 2007

lec 7F.3

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

Planar Graphs

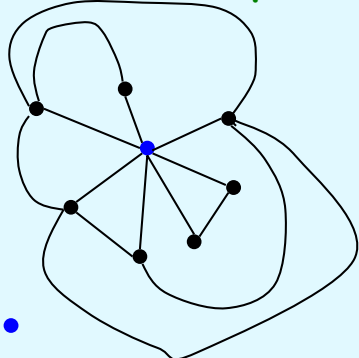


Copyright © Albert R. Meyer, 2007. All rights reserved. March 23, 2007

lec 7F.4

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

Planar Graphs



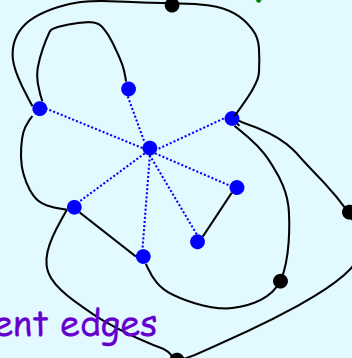
delete •

Copyright © Albert R. Meyer, 2007. All rights reserved. March 23, 2007

lec 7F.5

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

Planar Graphs



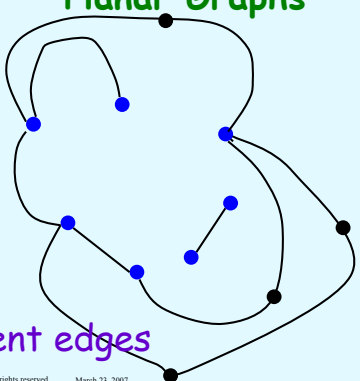
& incident edges

Copyright © Albert R. Meyer, 2007. All rights reserved. March 23, 2007

lec 7F.6

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

Planar Graphs



& incident edges

Copyright © Albert R. Meyer, 2007. All rights reserved. March 23, 2007 lec 7F.7

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

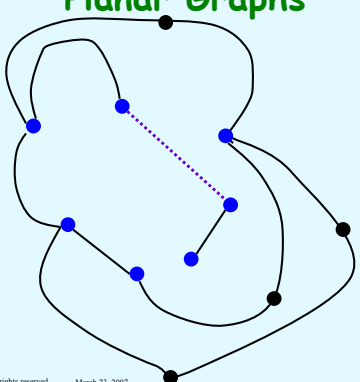
Planar Graphs

- then can connect any two of its adjacent vertices, ●, and stay planar:

Copyright © Albert R. Meyer, 2007. All rights reserved. March 23, 2007 lec 7F.8

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

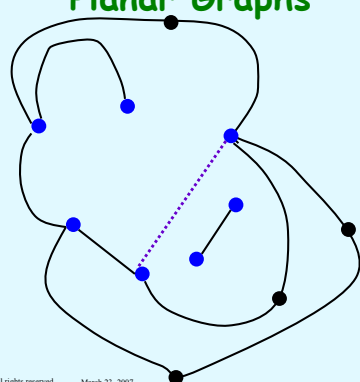
Planar Graphs



Copyright © Albert R. Meyer, 2007. All rights reserved. March 23, 2007 lec 7F.9

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

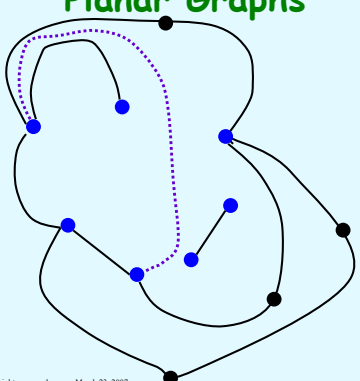
Planar Graphs



Copyright © Albert R. Meyer, 2007. All rights reserved. March 23, 2007 lec 7F.10

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

Planar Graphs



Copyright © Albert R. Meyer, 2007. All rights reserved. March 23, 2007 lec 7F.11

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

Planar Graphs

- merging adjacent vertices in a planar graph leaves a planar graph

Copyright © Albert R. Meyer, 2007. All rights reserved. March 23, 2007 lec 7F.13

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

Planar Graphs

Copyright © Albert R. Meyer, 2007. All rights reserved. March 23, 2007 lec 7F.14

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

Planar Graphs

Copyright © Albert R. Meyer, 2007. All rights reserved. March 23, 2007 lec 7F.15

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

Planar Graphs

Copyright © Albert R. Meyer, 2007. All rights reserved. March 23, 2007 lec 7F.16

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

Planar Graphs

Copyright © Albert R. Meyer, 2007. All rights reserved. March 23, 2007 lec 7F.17

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

Planar Graphs

Copyright © Albert R. Meyer, 2007. All rights reserved. March 23, 2007 lec 7F.18

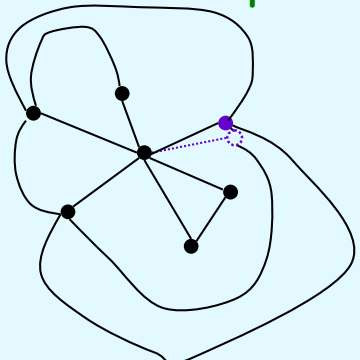
6	9	13	7
12		10	5
3	1	4	14
15	8	11	2

Planar Graphs

Copyright © Albert R. Meyer, 2007. All rights reserved. March 23, 2007 lec 7F.19

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

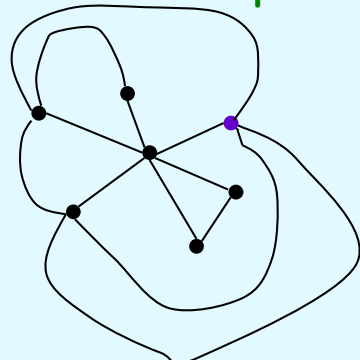
Planar Graphs



Copyright © Albert R. Meyer, 2007. All rights reserved. March 23, 2007 lec 7F.20

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

Planar Graphs



Copyright © Albert R. Meyer, 2007. All rights reserved. March 23, 2007 lec 7F.21

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

5-Color Theorem

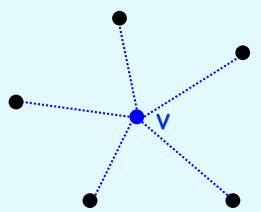
By induction on # vertices:
 case 1: vertex of $\deg \leq 4$.
 remove vertex, v ,
 5-color remainder, then
 enough colors left
 to color v . OK

Copyright © Albert R. Meyer, 2007. All rights reserved. March 23, 2007 lec 7F.22

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

5-Color Theorem

case 2: vertex v of $\deg = 5$.

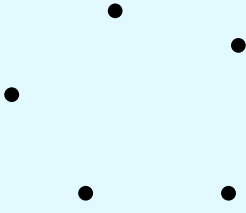


Copyright © Albert R. Meyer, 2007. All rights reserved. March 23, 2007 lec 7F.23

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

5-Color Theorem

remove v

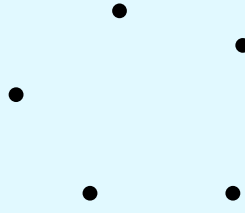


Copyright © Albert R. Meyer, 2007. All rights reserved. March 23, 2007 lec 7F.24

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

5-Color Theorem

remaining 5 not all adjacent



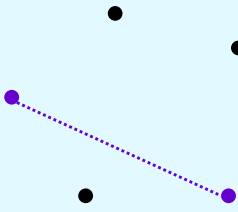
else would have K_5

Copyright © Albert R. Meyer, 2007. All rights reserved. March 23, 2007 lec 7F.25

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

5-Color Theorem

pick 2 not adjacent



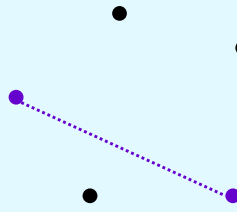
add edge (still planar)

Copyright © Albert R. Meyer, 2007. All rights reserved. March 23, 2007 lec 7F.26

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

5-Color Theorem

merge (still planar)

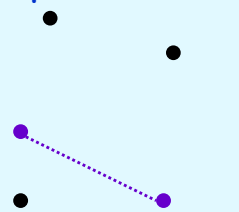


Copyright © Albert R. Meyer, 2007. All rights reserved. March 23, 2007 lec 7F.27

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

5-Color Theorem

merge (still planar)

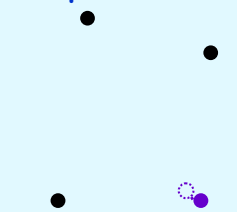


Copyright © Albert R. Meyer, 2007. All rights reserved. March 23, 2007 lec 7F.28

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

5-Color Theorem

merge (still planar)

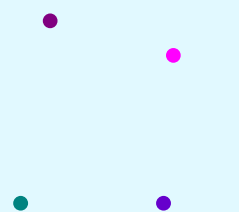


Copyright © Albert R. Meyer, 2007. All rights reserved. March 23, 2007 lec 7F.29

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

5-Color Theorem

now 5-color

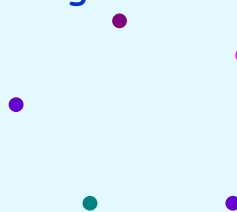


Copyright © Albert R. Meyer, 2007. All rights reserved. March 23, 2007 lec 7F.30

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

5-Color Theorem

now unmerge

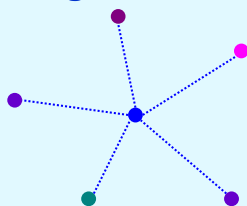


Copyright © Albert R. Meyer, 2007. All rights reserved. March 23, 2007 lec 7F.31

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

5-Color Theorem

now unmerge, restore v



only 4 colors adjacent to v , so **OK**

Copyright © Albert R. Meyer, 2007. All rights reserved. March 23, 2007

lec 7F.32

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

Benés Network

see

<http://theory.csail.mit.edu/classes/6.042/spring07/slides6f.pdf>

Copyright © Albert R. Meyer, 2007. All rights reserved. March 23, 2007

lec 7F.48

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

Team Problems

Problems 1-3

Copyright © Albert R. Meyer, 2007. All rights reserved. March 23, 2007

lec 7F.61

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

Mathematics for Computer Science

MIT 6.042J/18.062J

Prime Factorization Congruences

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 2, 2007

lec 8M.1

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

Prime Divisibility

Lemma: If p is prime, and
 $p \mid a \cdot b$,

then $p \mid a$ or $p \mid b$.

pf: in earlier lecture. follows from

$$\gcd(p, a) = xa + yp$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 2, 2007

lec 8M.3

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

Prime Divisibility

Cor : If p is prime, and
 $p \mid a_1 \cdot a_2 \cdots a_m$
then $p \mid a_i$ for some i .

pf: By induction on m .

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 2, 2007

lec 8M.4

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

Unique Prime Factorization

Fundamental Theorem of Arithmetic

Every integer > 1 factors
uniquely into a weakly
increasing sequence of
primes.

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 2, 2007

lec 8M.5

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

Unique Prime Factorization

Fundamental Theorem of Arithmetic

Example:

$$61394323221 =$$

$$3 \cdot 3 \cdot 3 \cdot 7 \cdot 11 \cdot 11 \cdot 37 \cdot 37 \cdot 37 \cdot 53$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 2, 2007

lec 8M.6

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

Unique Prime Factorization

pf: suppose not. choose **smallest** $n > 1$:

$$n = p_1 \cdot p_2 \cdots p_k = q_1 \cdot q_2 \cdots q_m$$

$$p_1 \leq p_2 \leq \cdots \leq p_k$$

$$q_1 \leq q_2 \leq \cdots \leq q_m$$

can assume $q_1 < p_1$

so $q_1 \neq p_i$ all i

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 2, 2007

lec 8M.7

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

Unique Prime Factorization

pf: $n = p_1 \cdot p_2 \cdots p_k = q_1 \cdot q_2 \cdots q_m$
 now $p_1 | n$, so by Cor., $p_1 | q_i$.
 so $p_1 = q_i$ with $i > 1$.
 so $\underbrace{p_2 \cdots p_k}_{< n} = q_1 \cdot q_2 \cdots q_{i-1} \cdot q_{i+1} \cdots q_m$
 and $q_1 \neq p_2$

contradiction!

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 2, 2007

lec 8M.8

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

Unique Prime Factorization

Cor: if $n = p_1 \cdot p_2 \cdots p_k$,
 and $m | n$, then

$$m = p_{i_1} \cdot p_{i_2} \cdots p_{i_j}$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 2, 2007

lec 8M.9

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

Team Problem

Problem 1

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 2, 2007

lec 8M.10

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

Congruences

Def: $a \equiv b \pmod{n}$ iff $n | (a - b)$.

Lemma: If $a \equiv b \pmod{n}$, then
 $a + c \equiv b + c \pmod{n}$.

pf: $n | (a - b)$ implies
 $n | ((a + c) - (b + c))$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 2, 2007

lec 8M.11

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

Congruences

Lemma:

If $a \equiv b \pmod{n}$, then
 $a \cdot c \equiv b \cdot c \pmod{n}$.

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 2, 2007

lec 8M.13

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

Congruences

Lemma:

$$a \equiv \text{rem}(a, n) \pmod{n}$$

important: keeps (mod n)
 calculations in the range
 0 to n-1

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 2, 2007

lec 8M.14

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

Congruences

Cor: $a \equiv b \pmod{n}$ iff
 $\text{rem}(a,n) = \text{rem}(b,n)$

Cor: $a \equiv a \pmod{n}$.

If $a \equiv b$ & $b \equiv c \pmod{n}$,
 then $a \equiv c \pmod{n}$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 2, 2007

lec 8M.15

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

Congruences

So $\equiv \pmod{n}$ a lot like $=$.

main diff: can't cancel

$$4 \cdot 2 \equiv 1 \cdot 2 \pmod{6}$$

$$4 \not\equiv 1 \pmod{6}$$

No general cancellation

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 2, 2007

lec 8M.16

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

Relatively prime cancellation

If $\text{gcd}(k,n)=1$, then have k'
 $k \cdot k' \equiv 1 \pmod{n}$.

k' is an *inverse* mod n of k

pf: $sk + tn = 1$.

just let $k' = s$.

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 2, 2007

lec 8M.17

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

Relatively prime cancellation

Cor.

If $i \cdot k \equiv j \cdot k \pmod{n}$,

and $\text{gcd}(k,n) = 1$,

then $i \equiv j \pmod{n}$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 2, 2007

lec 8M.18

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

Fermat's Little Theorem

If p is prime & k not a multiple of p ,
 can cancel k . So

$$k, 2k, \dots, (p-1)k$$

are all different \pmod{p} .

So their remainders on division
 by p are all different \pmod{p} .

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 2, 2007

lec 8M.19

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

Fermat's Little Theorem

This means that

$\text{rem}(k, p), \text{rem}(2k, p), \dots, \text{rem}((p-1)k, p)$

must be a *permutation* of

$$1, 2, \dots, (p-1)$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 2, 2007

lec 8M.20

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

Fermat's Little Theorem

so $1 \cdot 2 \cdots (p-1) =$

$\text{rem}(k,p) \cdot \text{rem}(2k,p) \cdots \text{rem}((p-1)k,p)$

$\equiv (k) \cdot (2k) \cdots ((p-1)k) \pmod{p}$

$\equiv (k^{p-1}) \cdot 1 \cdot 2 \cdots (p-1) \pmod{p}$

so

$$1 \equiv k^{p-1} \pmod{p}$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 2, 2007

lec 8M.21

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

Team Problems

Problems 2–4

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 2, 2007

lec 8M.22

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

Euler's Theorem RSA encryption

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

Inverses mod n

Thm. If k is relatively prime to n , there is an inverse k'
 $k \cdot k' \equiv 1 \pmod{n}$

Cor.

OK to **cancel** (mod n)

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

The interval from 0 to n

$$[0, n) ::= \{0, 1, \dots, n-1\}$$

$$[0, n] ::= \{0, 1, \dots, n\}$$

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

Euler ϕ function

$\phi(n) ::= \# k \in [0, n)$ s.t.
 k rel. prime to n

$$\phi(7) = 6 \quad 1, 2, 3, 4, 5, 6$$

$$\phi(12) = 4 \quad 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11$$

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

Calculating ϕ

If p prime, everything from 1 to $p-1$ is rel. prime to p , so

$$\phi(p) = p - 1$$

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

Euler ϕ function

$\phi(49)?$

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, ..., 13, 14, 15, ..., 21, ...

every 7th number is divisible by 7

$$\text{so, } \phi(49) = 49 - 7$$

6	9	10	7
12	18	5	
3	1	4	14
15	8	11	2

Calculating ϕ

For $[0, p^k)$ every p th element is **not** rel. prime to p^k :

$0, 1, \dots, p-1, p, \dots, 2p, \dots, (p^{k-2})p, \dots, p^{k-1}$

$(1/p)p^k$ elements
not rel. prime to p^k

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 4, 2007

lec 8W.7

6	9	10	7
12	18	5	
3	1	4	14
15	8	11	2

Calculating ϕ

$$\phi(p^k) = p^k - p^{k-1}$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 4, 2007

lec 8W.8

6	9	10	7
12	18	5	
3	1	4	14
15	8	11	2

Calculating ϕ

For $1, 2, \dots, p-1, p, \dots, 2p, \dots, p^{k-1}, p^k$
every p th is **not** rel. prime to p^k

$$\phi(p^k) = p^k - p^{k-1}$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 4, 2007

lec 8W.9

6	9	10	7
12	18	5	
3	1	4	14
15	8	11	2

Calculating ϕ

Lemma :

For a, b relatively prime,

$$\phi(a \cdot b) = \phi(a) \cdot \phi(b)$$

pf: Pset 7 now;
another way in 3 weeks

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 4, 2007

lec 8W.10

6	9	10	7
12	18	5	
3	1	4	14
15	8	11	2

Euler's Theorem

For k relatively prime to n ,

$$k^{\phi(n)} \equiv 1 \pmod{n}$$

Fermat Thm a special case.
Euler proof essentially
same as Fermat:



Copyright © Albert R. Meyer, 2007. All rights reserved.

April 4, 2007

lec 8W.11

6	9	10	7
12	18	5	
3	1	4	14
15	8	11	2

Proof of Euler's Thm

For k relatively prime to n , let
 $r ::= \phi(n)$ and

k_1, \dots, k_r
the integers in $[0, n)$ relatively
prime to n . Then
 $\text{rem}(k_1 k, n), \text{rem}(k_2 k, n), \dots, \text{rem}(k_r k, n)$
is a permutation of k_1, \dots, k_r .
pf: cancel $k \pmod{n}$.

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 4, 2007

lec 8W.12

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

Proof of Euler's Thm

So

$$\begin{aligned} k_1 \dots k_r &= \text{rem}(k_1 k, n) \dots \text{rem}(k_r k, n) \\ &\equiv k_1 k \dots k_r k \pmod{n} \\ &= k^r \cdot k_1 \dots k_r \pmod{n} \end{aligned}$$

But OK to cancel k_1, \dots, k_r , so
 $1 \equiv k^r \pmod{n}$.

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 4, 2007

lec 8W.13

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

RSA Public Key Encryption



Copyright © Albert R. Meyer, 2007. All rights reserved.

April 4, 2007

lec 8W.14

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

Beforehand

- receiver generates primes p, q
- $n ::= pq$
- selects e rel. prime to $(p-1)(q-1)$
- $(e, n) ::=$ public key, publishes it
- finds d , inverse mod $(p-1)(q-1)$ of e
- d is secret key, keeps hidden

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 4, 2007

lec 8W.15

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

Receiver's abilities

- find two large primes p, q
 - ok because: lots of primes
 - fast test for primality
- find e rel. prime to $(p-1)(q-1)$
 - ok: lots of rel. prime nums
 - gcd easy to compute
- find inverse of e
 - easy using Pulverizer or Euler

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 4, 2007

lec 8W.16

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

RSA

- Encoding message m :
 send $m' ::= \text{rem}(m^e, n)$
- Decoding m' :
 receiver computes
 $\text{rem}((m')^d, n) = m$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 4, 2007

lec 8W.17

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

Why does this work?

...explained in
 Team Problem

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 4, 2007

lec 8W.18



1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Why is it secure?

- easy to break *if* can factor n
(find d same way receiver did)
- conversely, from d can factor n
- but factoring appears hard
- has withstood 25 years of attacks

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 4, 2007

lec 8W.19



1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Team Problems

Problems 1&2

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 4, 2007

lec 8W.20



Mathematics for Computer Science
MIT 6.042J/18.062J

Sums & Money

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 6, 2007

lec 8F.1



C. F. Gauss



Picture source: <http://www-groups.dcs.st-and.ac.uk/~history/PictDisplay/Gauss.html>

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 6, 2007

lec 8F.2



Sum for Children

$$\begin{array}{rcl} 89 & + & 102 + 115 + 128 + 141 + \\ 154 & + & \dots + \\ 193 & + & \dots + \\ 232 & + & \dots + \\ 323 & + & \dots + \\ 414 & + & \dots + 453 + 466 \end{array}$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 6, 2007

lec 8F.3



Sum for Children

Nine-year old Gauss saw
30 numbers, each 13 greater
than the previous one.
(So the story goes.)

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 6, 2007

lec 8F.4



Sum for Children

$$\begin{array}{rcl} 1^{\text{st}} + 30^{\text{th}} & = & 89 + 466 = 555 \\ 2^{\text{nd}} + 29^{\text{th}} & = & \\ (1^{\text{st}}+13) + (30^{\text{th}}-13) & = & 555 \\ 3^{\text{rd}} + 28^{\text{th}} & = & \\ (2^{\text{nd}}+13) + (29^{\text{th}}-13) & = & 555 \\ & \vdots & \end{array}$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 6, 2007

lec 8F.5



Sum for Children

Sum of k^{th} term and $(31-k)^{\text{th}}$ term
is **invariant!** 15 pairs of terms, so
Total = $555 \cdot 15$
= $(1^{\text{st}} + \text{last}) \cdot (\# \text{ terms}/2)$
= $(1^{\text{st}} + \text{last})/2 \cdot (\# \text{ terms})$
average term

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 6, 2007

lec 8F.6

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

Sum for Children

Example:

$$1 + 2 + \dots + (n-1) + n = \frac{(1+n)n}{2}$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 6, 2007

lec 8F.7

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

Geometric Series

$$G_n ::= 1 + x + x^2 + \dots + x^{n-1} + x^n$$

$$xG_n = x + x^2 + x^3 + \dots + x^n + x^{n+1}$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 6, 2007

lec 8F.8

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

Geometric Series

$$G_n ::= 1 + \cancel{x} + \cancel{x^2} + \dots + \cancel{x^{n-1}} + \cancel{x^n}$$

$$xG_n = \cancel{x} + \cancel{x^2} + \cancel{x^3} + \dots + \cancel{x^n} + x^{n+1}$$

$$G_n - xG_n = 1 - x^{n+1}$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 6, 2007

lec 8F.9

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

Geometric Series

$$G_n ::= 1 + \cancel{x} + \cancel{x^2} + \dots + \cancel{x^{n-1}} + \cancel{x^n}$$

$$xG_n = \cancel{x} + \cancel{x^2} + \cancel{x^3} + \dots + \cancel{x^n} + x^{n+1}$$

$$G_n - xG_n = 1 - x^{n+1}$$

$$G_n = \frac{1 - x^{n+1}}{1 - x}$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 6, 2007

lec 8F.10

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

Geometric Series

$$G_n = \frac{1 - x^{n+1}}{1 - x}$$

Consider *infinite* sum (series)

$$1 + x + x^2 + \dots + x^{n-1} + x^n + \dots = \sum_{i=0}^{\infty} x^i$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 6, 2007

lec 8F.11

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

Infinite Geometric Series

$$G_n = \frac{1 - x^{n+1}}{1 - x}$$

$$\lim_{n \rightarrow \infty} G_n = \frac{1 - \lim_{n \rightarrow \infty} x^{n+1}}{1 - x} = \frac{1}{1 - x}$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 6, 2007

lec 8F.12

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

Infinite Geometric Series

$$\sum_{i=0}^{\infty} x^i = \frac{1}{1-x}$$

for $|x| < 1$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 6, 2007

lec 8F.13

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

Team Problem

Problem 1

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 6, 2007

lec 8F.14

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

The future value of \$\$

I will pay you \$100 in 1 year,
if you will pay me \$X now.

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 6, 2007

lec 8F.15

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

The future value of \$\$

My bank will pay me 3% interest.

define *bankrate*

$b ::= 1.03$

-- bank increases my \$ by this
factor in 1 year.

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 6, 2007

lec 8F.16

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

The future value of \$\$

If I deposit your \$X now,
I will have $b \cdot X$ in 1 year.

So I won't lose money as long as

$$b \cdot X \geq 100.$$

$$X \geq \$100/1.03 \approx \$97.09$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 6, 2007

lec 8F.17

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

The future value of \$\$

- \$1 in 1 year is worth \$0.9709 now.
- \$r last year is worth \$1 today,
where $r ::= 1/b$.
- So \$n paid in 2 years is worth
\$nr paid in 1 year, and is worth
\$nr² today.

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 6, 2007

lec 8F.18

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

The future value of \$\$

$\$n$ paid k years from now
is worth $\$n \cdot r^k$ today
where $r ::= 1/\text{bankrate}$.

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 6, 2007

lec 8F.19

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

Annuities

I pay you $\$100/\text{year}$ for 10 years,
if you will pay me $\$Y$ now.

I *can't lose* if you pay me

$$\begin{aligned} &100r + 100r^2 + 100r^3 + \dots + 100r^{10} \\ &= 100r(1 + r + \dots + r^9) \\ &= 100r(1 - r^{10})/(1 - r) = \$853.02 \end{aligned}$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 6, 2007

lec 8F.20

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

Annuities

I pay you $\$100/\text{year}$ for 10 years,
if you will pay me $\$853.02$.

QUICKIE: If bankrates unexpectedly
increase in the next few years,

- A. You come out ahead
- B. The deal stays fair
- C. I come out ahead

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 6, 2007

lec 8F.21

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

Manipulating Sums

$$\frac{d}{dx} \left(\sum_{i=0}^n x^i \right) = \frac{d}{dx} \left(\frac{1 - x^{n+1}}{1 - x} \right)$$

$$\sum_{i=0}^n i x^{i-1} = \frac{1}{x} \sum_{i=1}^n i x^i = \frac{d}{dx} \left(\frac{1 - x^{n+1}}{1 - x} \right)$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 6, 2007

lec 8F.22

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

Manipulating Sums

$$\sum_{i=1}^n i x^{i-1} = \frac{x - (n+1)x^{n+1} + nx^{n+2}}{(1-x)^2}$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 6, 2007

lec 8F.23

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

Team Problems

Problems

2&3

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 6, 2007

lec 8F.24

6	9	13	7
12		10	5
3	1	16	14
15	8	11	2

Harmonic Series, Integral Method

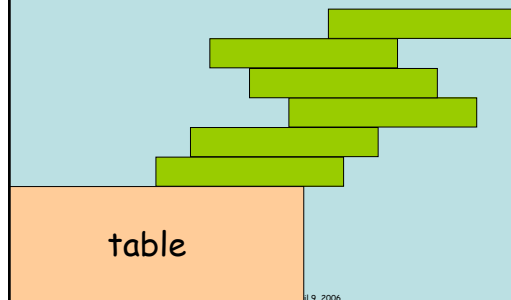
Copyright © Albert R. Meyer, 2007. All rights reserved.

April 9, 2006

lec 9M.1

6	9	13	7
12		10	5
3	1	16	14
15	8	11	2

Book Stacking



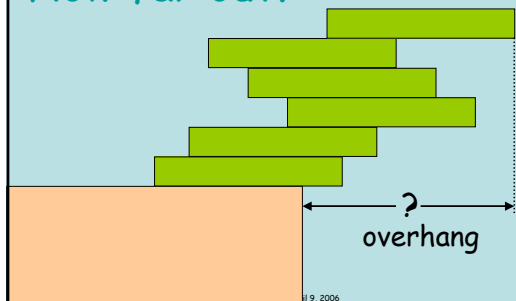
4/9, 2006

lec 9M.2

6	9	13	7
12		10	5
3	1	16	14
15	8	11	2

Book Stacking

How far out?



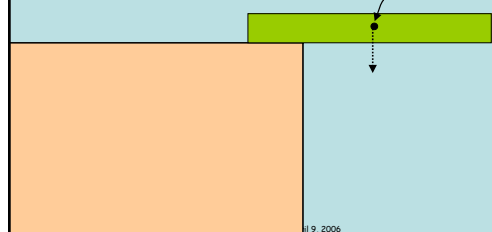
4/9, 2006

lec 9M.3

6	9	13	7
12		10	5
3	1	16	14
15	8	11	2

Book Stacking

One book



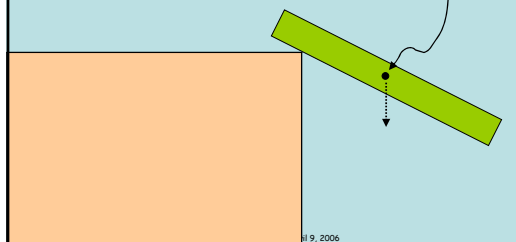
4/9, 2006

lec 9M.4

6	9	13	7
12		10	5
3	1	16	14
15	8	11	2

Book Stacking

One book



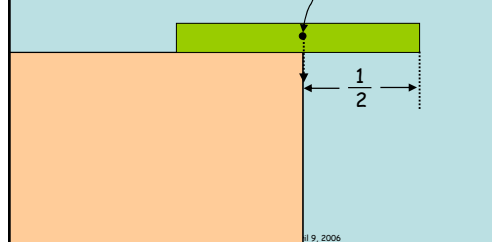
4/9, 2006

lec 9M.5

6	9	13	7
12		10	5
3	1	16	14
15	8	11	2

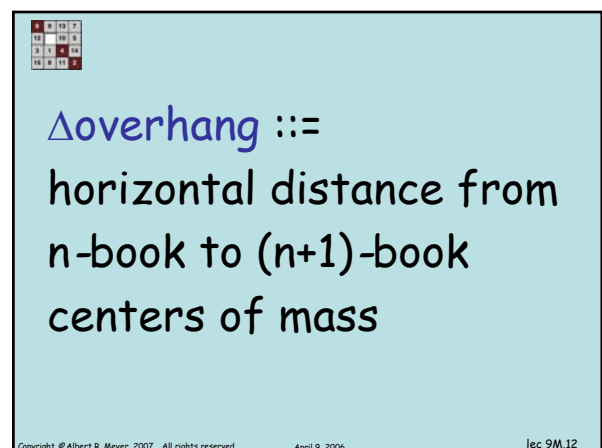
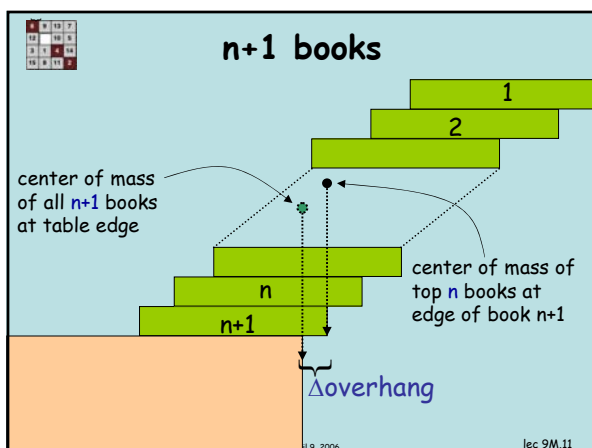
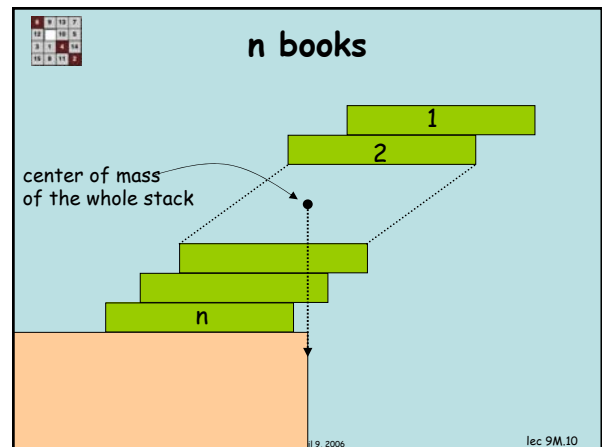
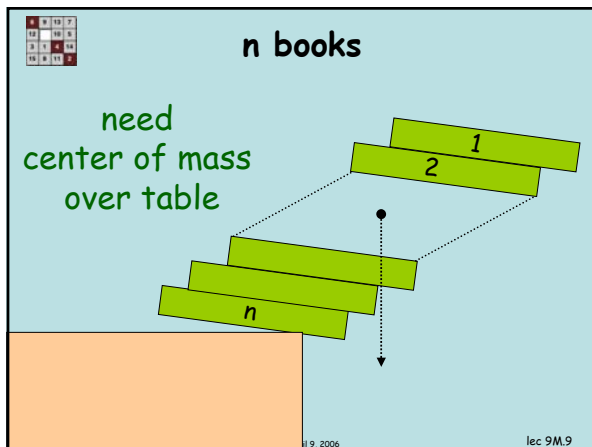
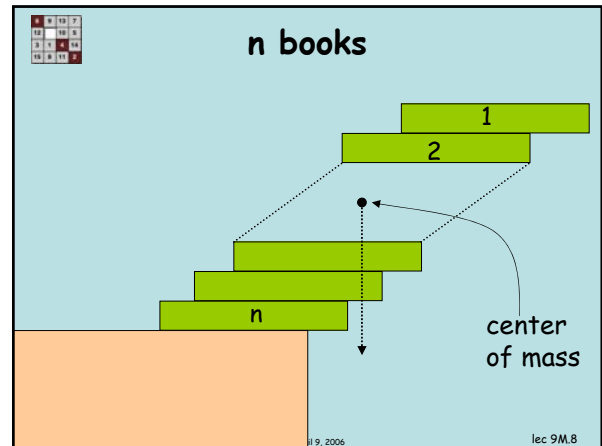
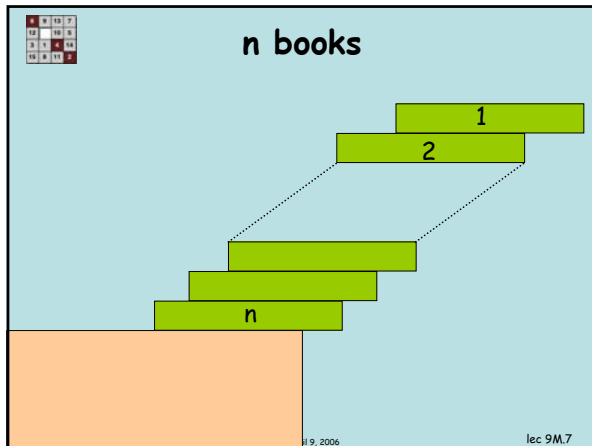
Book Stacking


One book



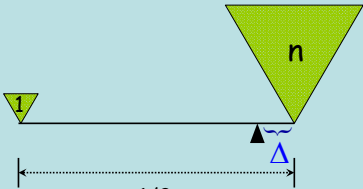
4/9, 2006

lec 9M.6






Δ overhang

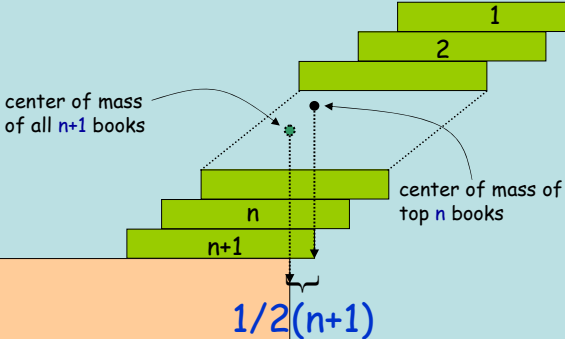


$$\Delta = \frac{1/2}{n+1} = \frac{1}{2(n+1)}$$

Copyright © Albert R. Meyer, 2007. All rights reserved. April 9, 2006 lec 9M.13



$n+1$ books




center of mass of all $n+1$ books

center of mass of top n books

$1/2(n+1)$

Copyright © Albert R. Meyer, 2007. All rights reserved. April 9, 2006 lec 9M.16



Book stacking summary


$B_n ::=$ overhang of n books

$B_1 = 1/2$

$B_{n+1} = B_n + \frac{1}{2(n+1)}$

$B_n = \frac{1}{2} \left(1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n} \right)$

Copyright © Albert R. Meyer, 2007. All rights reserved. April 9, 2006 lec 9M.17




$$H_n ::= 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n}$$

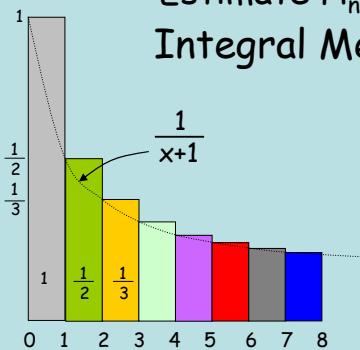
n^{th} Harmonic number

$B_n = H_n/2$

Copyright © Albert R. Meyer, 2007. All rights reserved. April 9, 2006 lec 9M.18



Estimate H_n : Integral Method




$\frac{1}{x+1}$

1, $\frac{1}{2}$, $\frac{1}{3}$

0 1 2 3 4 5 6 7 8

Copyright © Albert R. Meyer, 2007. All rights reserved. April 9, 2006 lec 9M.19



$$\int_0^n \frac{1}{x+1} dx \leq 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n}$$

$$\int_1^{n+1} \frac{1}{x} dx \leq H_n$$

$\ln(n+1) \leq H_n$

Copyright © Albert R. Meyer, 2007. All rights reserved. April 9, 2006 lec 9M.20

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

Book stacking

Now $H_n \rightarrow \infty$ as $n \rightarrow \infty$, so
overhang can be as big desired

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 9, 2006

lec 9M.21

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

Book stacking

for overhang 3, need $B_n \geq 3$

$$H_n \geq 6$$

integral bound: $\ln(n+1) \geq 6$

so can do with $n \geq \lceil e^6 - 1 \rceil = 403$ books

actually calculate H_n :

227 books are enough.

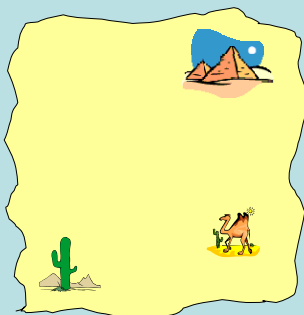
Copyright © Albert R. Meyer, 2007. All rights reserved.

April 9, 2006

lec 9M.22

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

Crossing a Desert



How big a desert can the truck cross?

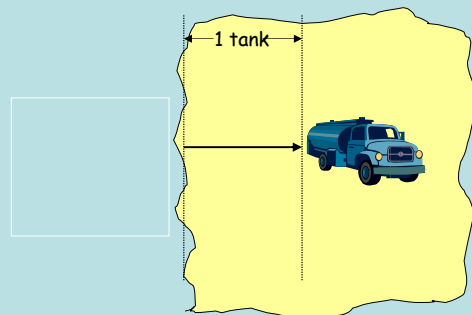
Copyright © Albert R. Meyer, 2007. All rights reserved.

April 9, 2006

lec 9M.24

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

1 Tank of Gas



$D_1 ::= \text{max distance on 1 tank} = 1$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 9, 2006

lec 9M.25

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

$D_n ::=$
max distance into the
desert using n tanks
of gas from the depot

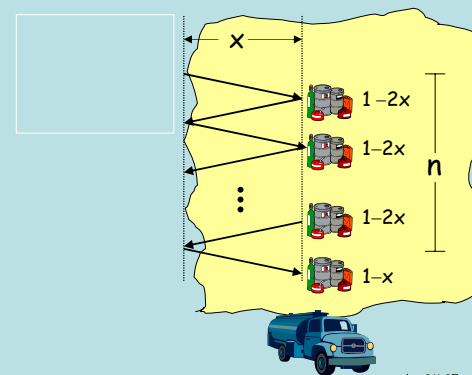
Copyright © Albert R. Meyer, 2007. All rights reserved.

April 9, 2006

lec 9M.26

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


$n+1$ Tanks of Gas



Copyright © Albert R. Meyer, 2007. All rights reserved.

April 9, 2006


lec 9M.27

 **n+1 Tanks of Gas**


So have:
grow depot at x
to be n tanks;
continue from
 x with n tank
method.


x

$(1-2x)n + (1-x)$



Copyright © Albert R. Meyer, 2007. All rights reserved. April 9, 2006 lec 9M.28


 depot at x

 Set $(1-2x)n + (1-x) = n$.

Then using n tank strategy
from position x , gives

$$D_{n+1} = D_n + x$$


Copyright © Albert R. Meyer, 2007. All rights reserved. April 9, 2006 lec 9M.29

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

$$x = \frac{1}{2n+1}$$

$$D_{n+1} = D_n + \frac{1}{2n+1}$$

Copyright © Albert R. Meyer, 2007. All rights reserved. April 9, 2006 lec 9M.30


 $D_n = 1 + \frac{1}{3} + \frac{1}{5} + \dots + \frac{1}{2n-1}$

$$\int_0^n \frac{1}{2(x+1)-1} dx \leq D_n$$

$$\frac{\ln(2n+1)}{2} \leq D_n$$

Can cross any desert!

Copyright © Albert R. Meyer, 2007. All rights reserved. April 9, 2006 lec 9M.31

 Team Problems

Problems 1–3

Copyright © Albert R. Meyer, 2007. All rights reserved. April 9, 2006 lec 9M.32



Stirling's formula, Asymptotics

Closed form for $n!$ Factorial defines a **product**:

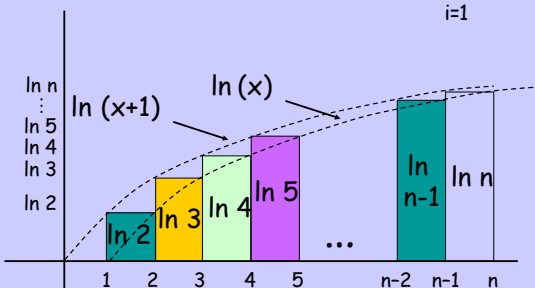
$$n! ::= 1 \times 2 \times 3 \times \dots \times (n-1) \times n = \prod_{i=1}^n i$$

Turn product into a **sum** taking logs:

$$\begin{aligned} \ln(n!) &= \ln(1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n) \\ &= \ln 1 + \ln 2 + \dots + \ln(n-1) + \ln(n) \\ &= \sum_{i=1}^n \ln(i) \end{aligned}$$



Integral Method

Integral method to bound $\sum_{i=1}^n \ln i$ Integral Method on $\ln(n!)$

$$\int_1^n \ln(x) dx \leq \sum_{i=1}^n \ln(i) \leq \int_0^n \ln(x+1) dx$$

Integral Method on $\ln(n!)$ *Reminder:*

$$\int \ln x dx = x \ln\left(\frac{x}{e}\right)$$

Integral Method on $\ln(n!)$

$$\int_1^n \ln(x) dx \leq \sum_{i=1}^n \ln(i) \leq \int_0^n \ln(x+1) dx$$

$$n \ln(n/e) + 1 \leq \sum \ln(i) \leq (n+1) \ln((n+1)/e) + 1$$

so guess: $\sum_{i=1}^n \ln(i) \approx \left(n + \frac{1}{2}\right) \ln\left(\frac{n}{e}\right)$



Integral Method

$$\sum_{i=1}^n \ln(i) \approx \left(n + \frac{1}{2}\right) \ln\left(\frac{n}{e}\right)$$

exponentiating:

$$n! \approx \sqrt{n/e} \left(\frac{n}{e}\right)^n$$

Copyright © Albert Meyer, 2007. All rights reserved.

April 11, 2007

lec 9W.7



Stirling's Formula

A tighter approximation:

$$n! \sim \sqrt{2\pi n} \left(\frac{n}{e}\right)^n$$

Copyright © Albert Meyer, 2007. All rights reserved.

April 11, 2007

lec 9W.8



Asymptotic Equivalence

Def. $f(n) \sim g(n)$

iff $\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = 1$

Copyright © Albert Meyer, 2007. All rights reserved.

April 11, 2007

lec 9W.9



Asymptotic Equivalence \sim

Example: $(n^2 + n) \sim n^2$

because

$$\begin{aligned} \lim_{n \rightarrow \infty} \frac{n^2 + n}{n^2} &= \lim_{n \rightarrow \infty} \left[\frac{n^2}{n^2} + \frac{n}{n^2} \right] \\ &= \lim_{n \rightarrow \infty} \left[1 + \frac{1}{n} \right] \\ &= 1 + \lim_{n \rightarrow \infty} \frac{1}{n} \\ &= 1 + 0 = 1 \end{aligned}$$

Copyright © Albert Meyer, 2007. All rights reserved.

April 11, 2007

lec 9W.10



Little Oh: $o(\cdot)$

Asymptotically smaller:

Def. $f(n) = o(g(n))$

iff $\lim_{n \rightarrow \infty} \frac{f(n)}{g(n)} = 0$

Copyright © Albert Meyer, 2007. All rights reserved.

April 11, 2007

lec 9W.14



Little Oh: $o(\cdot)$

$$n^2 = o(n^3)$$

because

$$\lim_{n \rightarrow \infty} \frac{n^2}{n^3} =$$

$$\lim_{n \rightarrow \infty} \frac{1}{n} = 0$$

Copyright © Albert Meyer, 2007. All rights reserved.

April 11, 2007

lec 9W.15

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

Big Oh: $O(\cdot)$

Asymptotic Order of Growth:

$$f(n) = O(g(n))$$

$$\limsup_{n \rightarrow \infty} \left(\frac{f(n)}{g(n)} \right) < \infty$$

a technicality -- ignore now

Copyright © Albert Meyer, 2007. All rights reserved.

April 11, 2007

lec 9W.16

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

Big Oh: $O(\cdot)$

$$3n^2 = O(n^2)$$

because

$$\lim_{n \rightarrow \infty} \frac{3n^2}{n^2} = 3 < \infty$$

Copyright © Albert Meyer, 2007. All rights reserved.

April 11, 2007

lec 9W.17

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

The Oh's

Lemma:

If $f = o(g)$ or $f \sim g$, then $f = O(g)$

$$\lim = 0 \text{ or } \lim = 1 \rightarrow \lim < \infty$$

Copyright © Albert Meyer, 2007. All rights reserved.

April 11, 2007

lec 9W.18

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

The Oh's

If $f = o(g)$, then $g \neq O(f)$

$$\lim \frac{f}{g} = 0 \rightarrow \lim \frac{g}{f} = \infty$$

Copyright © Albert Meyer, 2007. All rights reserved.

April 11, 2007

lec 9W.20

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

Big Oh: $O(\cdot)$

Equivalent definition:

$$f(n) = O(g(n))$$

$$\exists c, n_0 \geq 0 \forall n \geq n_0. |f(n)| \leq c \cdot g(n)$$

Copyright © Albert Meyer, 2007. All rights reserved.

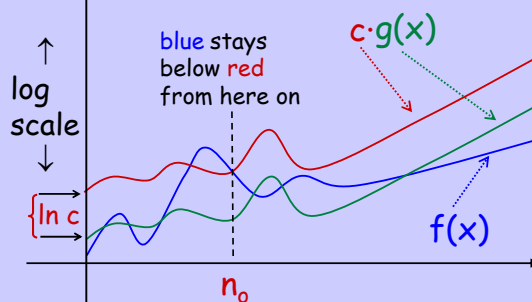
April 11, 2007

lec 9W.21

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

Big Oh: $O(\cdot)$

$$f(x) = O(g(x))$$



Copyright © Albert Meyer, 2003. All rights reserved.

October 16, 2003

L7-2.22



Team Problems

Problems 1&2

Copyright © Albert Meyer, 2007. All rights reserved.

April 11, 2007

lec 9W.23



Little Oh: $o(\cdot)$

Lemma: $x^a = o(x^b)$ for $a < b$

Proof: $\frac{x^a}{x^b} = \frac{1}{x^{b-a}}$ and $b - a > 0$

so as $x \rightarrow \infty$, $\frac{1}{x^{b-a}} \rightarrow 0$

Copyright © Albert Meyer, 2007. All rights reserved.

April 11, 2007

lec 9W.24



Little Oh: $o(\cdot)$

Lemma:

$\ln x = o(x^\delta)$
for $\delta > 0$.

Copyright © Albert Meyer, 2007. All rights reserved.

April 11, 2007

lec 9W.25



Little Oh: $o(\cdot)$

Lemma: $\ln x = o(x^\delta)$ for $\delta > 0$.

Proof: $\frac{1}{y} \leq y$ for $y \geq 1$

$$\int_1^z \frac{1}{y} dy \leq \int_1^z y dy$$

$$\ln z \leq \frac{z^2 - 1}{2}$$

Copyright © Albert Meyer, 2007. All rights reserved.

April 11, 2007

lec 9W.26



Little Oh: $o(\cdot)$

Lemma: $\ln x = o(x^\delta)$ for $\delta > 0$.

Proof: $\ln z \leq \frac{z^2}{2}$, so let $z ::= \sqrt{x^\varepsilon}$

$$\frac{\varepsilon \ln x}{2} \leq \frac{x^\varepsilon}{2}$$

$$\ln x \leq \frac{x^\varepsilon}{\varepsilon} = o(x^\delta) \text{ for } \delta > \varepsilon.$$

Copyright © Albert Meyer, 2007. All rights reserved.

April 11, 2007

lec 9W.28



Little Oh: $o(\cdot)$

Other proofs:
L'Hopital's Rule,
McLaurin Series
(see a Calculus text)

Copyright © Albert Meyer, 2007. All rights reserved.

April 11, 2007

lec 9W.30

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Theta: $\Theta(\cdot)$

Same Order of Growth:

$$f(n) = \Theta(g(n))$$

$$f(n)=O(g(n)) \text{ and } g(n)=O(f(n))$$

Copyright © Albert Meyer, 2007 All rights reserved.

April 11, 2007

lec 9W.31

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Big Oh **Mistakes**

$f = O(g)$ defines a relation " $= O(\cdot)$ "

Don't write $O(g) = f$.

Otherwise: $x = O(x)$, so $O(x) = x$.

But $2x = O(x)$, so

$$2x = O(x) = x,$$

therefore $2x = x$.

Nonsense!

Copyright © Albert Meyer, 2007 All rights reserved.

April 11, 2007

lec 9W.33

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Big Oh Mistakes

False Lemma: $\sum_{i=1}^n i = O(n)$

Of course really:

$$\sum_{i=1}^n i = \Theta(n^2)$$

Copyright © Albert Meyer, 2007 All rights reserved.

April 11, 2007

lec 9W.35

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Big Oh Mistakes

False Lemma: $\sum_{i=1}^n i = O(n)$

false proof:

$$0 = O(1), 1 = O(1), 2 = O(1), \dots$$

So each $i = O(1)$. So

$$\begin{aligned} \sum_{i=1}^n i &= O(1) + O(1) + \dots + O(1) \\ &= n \cdot O(1) = O(n). \end{aligned}$$

Copyright © Albert Meyer, 2007 All rights reserved.

April 11, 2007

lec 9W.36

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Team Problems

Problems 3&4

Copyright © Albert Meyer, 2007 All rights reserved.

April 11, 2007

lec 9W.37

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

Counting

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

Counting in Gambling

A pair of Jacks is



what *fraction* of poker hands?
(*probability* of a pair of Jacks)

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

Counting in Algorithms

- How many comparisons are needed to *sort* n numbers?
- How many multiplications to compute d^n ?

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

Counting in Games



- How many different configurations for a Rubik's cube?



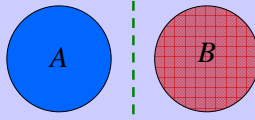
- How many different chess positions after n moves?



- How many weighings to find the one counterfeit among 12 coins?

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

Sum Rule



If sets A and B are **disjoint**, then

$$|A \cup B| = |A| + |B|$$

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

The Sum Rule

- Class has 43 women, 54 men so total enrollment = $43 + 54 = 97$
- 26 lower case letters, 26 upper case letters, and 10 digits, so total characters = $26+26+10 = 62$

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

The Product Rule

If there are 4 boys and 3 girls, there are possible
 $4 \times 3 = 12$
 married couples.

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 13, 2007

lec 9F.8

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

Product Rule

If $|A| = m$ and $|T| = n$, then
 $|A \times T| = mn.$

$$A = \{a, b, c, d\}, \quad T = \{1, 2, 3\}$$

$$A \times T = \{ (a,1), (a,2), (a,3), \\ (b,1), (b,2), (b,3), \\ (c,1), (c,2), (c,3), \\ (d,1), (d,2), (d,3) \}$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 13, 2007

lec 9F.9

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

Product Rule: Counting Strings

The number of length-4 strings
 from alphabet $B ::= \{0,1\}$

$$= |B \times B \times B \times B| \\ = 2 \cdot 2 \cdot 2 \cdot 2 = 2^4$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 13, 2007

lec 9F.10

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

Product Rule: Counting Strings

The number of length- n strings
 from an alphabet of size m is
 $m^n.$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 13, 2007

lec 9F.11

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

Example: Counting Passwords

- between 6 & 8 characters long
- starts with a letter
- case sensitive
- other characters: digits or letters

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 13, 2007

lec 9F.12

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

Counting Passwords

$$L ::= \{a, b, A, z, A, B, A, Z\}$$

$$D ::= \{0, 1, A, 9\}$$

$$P_n ::= \text{length } n \text{ passwords}$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 13, 2007

lec 9F.13

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

Counting Passwords

$$L ::= \{a, b, A, z, A, B, A, Z\}$$

$$D ::= \{0, 1, A, 9\}$$

$$P_6 =$$

$$L \times (L \cup D) \times (L \cup D) \times (L \cup D) \times (L \cup D) \times (L \cup D) \\ = L \times (L \cup D)^5$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 13, 2007

lec 9F.14

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

Counting Passwords

$$L ::= \{a, b, A, z, A, B, A, Z\}$$

$$D ::= \{0, 1, A, 9\}$$

$$P_n ::= \text{length } n \text{ passwords}$$

$$= L \times (L \cup D)^{n-1}$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 13, 2007

lec 9F.15

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

Counting Passwords

$$\begin{aligned} |L \times (L \cup D)^{n-1}| &= |L| \cdot |L \cup D|^{n-1} \\ &= |L| \cdot (|L| + |D|)^{n-1} \\ &= 52 \cdot 62^{n-1} \end{aligned}$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 13, 2007

lec 9F.16

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

Counting Passwords

The set of Passwords:

$$P = P_6 \cup P_7 \cup P_8$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 13, 2007

lec 9F.17

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

Counting Passwords

$$\begin{aligned} |P| &= |P_6| + |P_7| + |P_8| \\ &= 52 \cdot 62^5 + 52 \cdot 62^6 + 52 \cdot 62^7 \\ &= 186125210680448 \\ &\approx 19 \cdot 10^{14} \end{aligned}$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 13, 2007

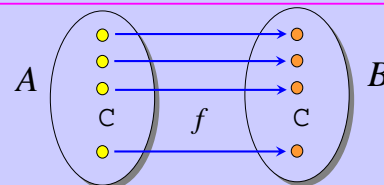
lec 9F.18

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

Mapping Rule: Bijections

If f is a **bijection** from A to B ,

then $|A| = |B|$



Copyright © Albert R. Meyer, 2007. All rights reserved.

April 13, 2007

lec 9F.21



Size of the Power Set

How many subsets of finite set A ?

$H(A)$ = the power set of A

= the set of all subsets of A

for $A = \{a, b, c\}$,

$H(A) = \{\emptyset, \{a\}, \{b\}, \{c\},$

$\{a,b\}, \{a,c\}, \{b,c\}, \{a,b,c\}\}$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 13, 2007

lec 9F.22



Bijection: $H(A)$ and Binary Strings

$A: \{a_1, a_2, a_3, a_4, a_5, \dots, a_n\}$

subset: $\{a_1, a_3, a_4, \dots, a_n\}$

string: 1 0 1 1 0 ... 1

a bijection, so

$$|\{n\text{-bit binary strings}\}| = |H(A)| = 2^n$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 13, 2007

lec 9F.23



Counting Doughnut Selections

five kinds of doughnuts

select a dozen:

 (none)    
 chocolate lemon-filled sugar glazed plain

$A ::=$ all selections of a dozen doughnuts

Copyright © Albert R. Meyer, 2007. All rights reserved.






April 13, 2007

lec 9F.24



Bit Strings with four 1's

$B ::=$ 16-bit words with four 1's, e.g.

0011000000100100
 00 1 1 000000 1 00 1 00
    
 chocolate lemon-filled sugar glazed plain

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 13, 2007

lec 9F.25



Bijection from A to B

c chocolate, l lemon, s sugar, g glazed, p plain

maps to

$0^c 10^l 10^s 10^g 10^p$

$$|A| = |B|$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 13, 2007

lec 9F.26



Team Problems

Problems

1.3

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 13, 2007

lec 9F.27



Generalized Counting Rules



Pigeonhole Principle

Mapping Rule:

If \exists **injection** A to B , then $|A| \leq |B|$.

If $|A| > |B|$, then
no injection from A to B .

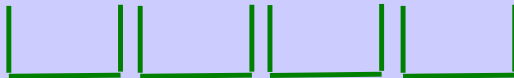


Pigeonhole Principle

If **more** pigeons



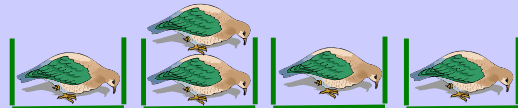
than pigeonholes,



Pigeonhole Principle

then **some hole** must have

\geq **two** pigeons!



Example: 5 Card Draw

Set of 5 cards:
must have ≥ 2
with the **same suit**.



5 Card Draw

5 cards
(pigeons)



4 suits
(holes)



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

10 Card Draw

10 cards: how many have the same suit?

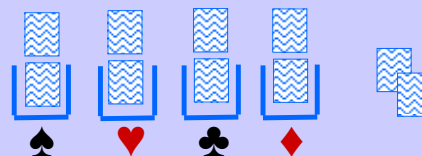
Copyright © Albert R. Meyer, 2007. All rights reserved.

April 18, 2007

lec 10W.7

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

10 Card Draw



Cannot have < 3 cards in every hole.

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 18, 2007

lec 10W.8

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

10 Card Draw

cards with same suit ≥ 3

$$\left\lceil \frac{10}{4} \right\rceil = 3 \text{ cards with same suit}$$

“ceiling,” means round up

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 18, 2007

lec 10W.9

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

Generalized Pigeonhole Principle

If n pigeons and h holes,
then some hole has at least

$$\left\lceil \frac{n}{h} \right\rceil \text{ pigeons.}$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

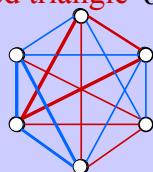
April 18, 2007

lec 10W.10

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

Colored Graph Claim

A 6-node complete graph with edges colored red or blue,
has *either* a red triangle or a blue triangle.



Copyright © Albert R. Meyer, 2007. All rights reserved.

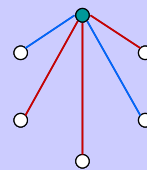
April 18, 2007

lec 10W.11

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

Colored Graph Claim: *proof*

Vertex of degree 5 has \geq
3 red or 3 blue incident edges.



Copyright © Albert R. Meyer, 2007. All rights reserved.

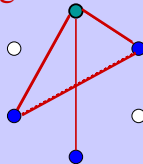
April 18, 2007

lec 10W.12

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

Proof

Say 3 red edges; if 2 of 3 endpoints are connected by red edge, then a red triangle is formed.



Copyright © Albert R. Meyer, 2007. All rights reserved.

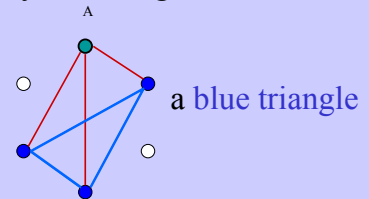
April 18, 2007

lec 10W.13

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

Proof

Otherwise, all 3 endpoints are connected by blue edges



Copyright © Albert R. Meyer, 2007. All rights reserved.

April 18, 2007

lec 10W.14

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

Generalized Product Rule

How many sequences of 5 students in 6.042?

$S ::= 6.042$ students, $|S| = 101$

~~$|\text{sequences of } 5| = 101^5$? NO!~~

We want

$|\text{sequences in } S^5 \text{ with no repeats.}|$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 18, 2007

lec 10W.15

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

Generalized Product Rule

$|\text{sequences in } S^5 \text{ with no repeats.}|$

101 choices for 1st student,
100 choices for 2nd student,
99 choices for 3rd student,
98 choices for 4th student,
97 choices for 5th student

so $101 \cdot 100 \cdot 99 \cdot 98 \cdot 97 = \frac{101!}{96!}$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 18, 2007

lec 10W.16

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

Generalized Product Rule

Q a set of length- k sequences. If there are:

n_1 possible 1st elements in sequences,

n_2 possible 2nd elements for each first entry,

n_3 possible 3rd elements for each 1st & 2nd,

\vdots

then, $|Q| = n_1 \cdot n_2 \cdot n_3 \cdots n_k$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 18, 2007

lec 10W.17

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

Division Rule

if function from A to B is k -to-1,
then

$$|A| = k |B|$$

(generalizes the Bijection Rule)

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 18, 2007

lec 10W.20

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

Division Rule

$$\frac{\#6.042 \text{ students} = \#6.042 \text{ students' fingers}}{10}$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 18, 2007

lec 10W.21

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

Counting Subsets

How many size 4 subsets of $\{1, 2, \dots, 13\}$?

Let $A ::=$ permutations of $\{1, 2, \dots, 13\}$

$B ::=$ size 4 subsets

map $a_1 a_2 a_3 a_4 a_5 \dots a_{12} a_{13}$ to $\{a_1, a_2, a_3, a_4\}$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 18, 2007

lec 10W.22

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

Counting Subsets

$a_2 a_4 a_3 a_1 a_5 \dots a_{12} a_{13}$ also maps to $\{a_1, a_2, a_3, a_4\}$

as does

$\underbrace{a_2 a_4 a_3 a_1}_{4!} \underbrace{a_{13} a_{12} \dots a_5}_{9!} \text{ 4!} \cdot 9! \text{-to-1}$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 18, 2007

lec 10W.23

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

Counting Subsets

$$13! = |A| = 4!9!|B|$$

So number of 4 element subsets is

$$\binom{13}{4} ::= \frac{13!}{4!9!}$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 18, 2007

lec 10W.24

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

Counting Subsets

Number of m element subsets of an n element set is

$$\binom{n}{m} ::= \frac{n!}{m!(n-m)!}$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 18, 2007

lec 10W.25

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

Team Problems

Problems
1–3

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 18, 2007

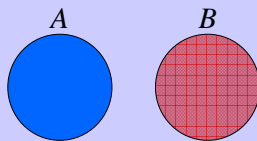
lec 10W.26

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

Sum Rule

If sets A and B are disjoint, then

$$|A \cup B| = |A| + |B|$$



What if A and B are **not disjoint**?

Copyright © Albert R. Meyer, 2007. All rights reserved.

April 18, 2007

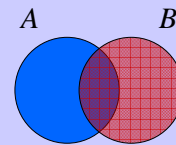
lec 10W.27

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

Inclusion-Exclusion (2 Sets)

For two arbitrary sets A and B

$$|A \cup B| = |A| + |B| - |A \cap B|$$



Copyright © Albert R. Meyer, 2007. All rights reserved.

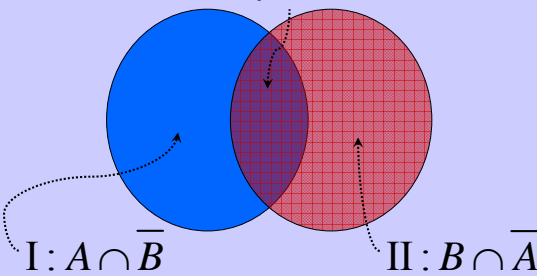
April 18, 2007

lec 10W.28

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

Inclusion-Exclusion (2 Sets)

III: $A \cap B$



I: $A \cap \bar{B}$

II: $B \cap \bar{A}$

Copyright © Albert R. Meyer, 2007. All rights reserved.

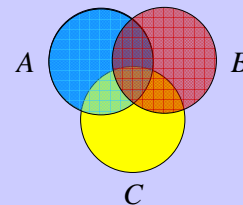
April 18, 2007

lec 10W.29

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

Inclusion-Exclusion (3 Sets)

$$\begin{aligned} |A \cup B \cup C| &= |A| + |B| + |C| \\ &\quad - |A \cap B| - |A \cap C| - |B \cap C| \\ &\quad + |A \cap B \cap C| \end{aligned}$$



Copyright © Albert R. Meyer, 2007. All rights reserved.

April 18, 2007

lec 10W.32

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

Team Problem

Problem 4

Copyright © Albert R. Meyer, 2007. All rights reserved.

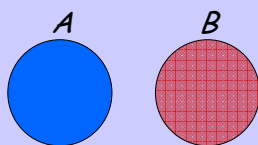
April 18, 2007

lec 10W.34

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

Sum Rule

$$|A \cup B| = |A| + |B|$$



for **disjoint** sets A, B

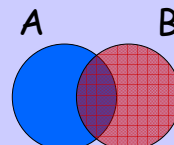
Copyright © 2007 by Albert R. Meyer. All rights reserved. April 20, 2007.

lec 10F.1

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

Sum Rule

$$|A \cup B| = ?$$



What if **not** disjoint?

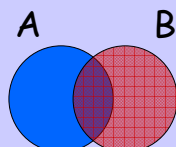
Copyright © 2007 by Albert R. Meyer. All rights reserved. April 20, 2007.

lec 10F.2

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

Inclusion-Exclusion

$$|A \cup B| = |A| + |B| - |A \cap B|$$



What if **not** disjoint?

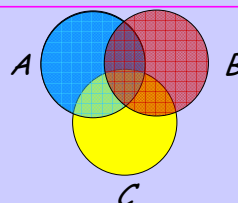
Copyright © 2007 by Albert R. Meyer. All rights reserved. April 20, 2007.

lec 10F.3

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

Inclusion-Exclusion (3 Sets)

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$



Copyright © 2007 by Albert R. Meyer. All rights reserved. April 20, 2007.

lec 10F.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

Tricks with Counting & Matching

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 20, 2007.

lec 10F.10

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

The Magic Trick

- Students **choose** 5 cards
- Chiyoun **reveals** 4 of them
- Jessica **announces** 5th card

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 20, 2007.

lec 10F.11

4	9	13	7
12	10	6	1
3	1	14	15
16	8	11	5

The Magic Trick

Let's do it!

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 20, 2007.

lec 10F.12

4	9	13	7
12	10	6	1
3	1	14	15
16	8	11	5

Chiyoun's Choices

- Decide **the order** of the 4 cards: $4! = 24$ orderings
-- but **48** cards remain
- Decide **which** 4 cards to list

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 20, 2007.

lec 10F.13

4	9	13	7
12	10	6	1
3	1	14	15
16	8	11	5

Match hands with 4-Card lists

5-card hands
(no order)



?



4-card lists
(ordered)



list must come
from hand

×

Which one to pick?

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 20, 2007.

lec 10F.14

4	9	13	7
12	10	6	1
3	1	14	15
16	8	11	5

Match hands with 4-Card lists

5-card hands
(no order)



?



4-card lists
(ordered)



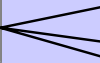
How can we ensure
consistency?

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 20, 2007.

lec 10F.15

4	9	13	7
12	10	6	1
3	1	14	15
16	8	11	5

Match hands with 4-Card lists



$$\deg = \binom{5}{4} \times 4! = 120$$

$$\deg = 52 - 4 = 48$$



Copyright © 2007 by Albert R. Meyer. All rights reserved. April 20, 2007.

lec 10F.21

4	9	13	7
12	10	6	1
3	1	14	15
16	8	11	5

Match hands with 4-Card lists

The graph is
degree-constrained
so there is a match that
Jessica and Chiyoun can use
—even works for bigger decks

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 20, 2007.

lec 10F.22

4	9	13	7
12	10	6	1
3	11	8	14
15	5	16	2

A Memorable Matching?

$$\binom{52}{5} = 2,598,960 \text{ hands to match to lists}$$

How will Jessica & Chiyoun learn them?

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 20, 2007.

lec 10F.23

4	9	13	7
12	10	6	1
3	11	8	14
15	5	16	2

Magic Trick Revealed (I)

Among 5 cards chosen:

at least 2 have the same suit
(Pigeonhole Principle)

Chiyoun lists one of them 1st

Aha! The first card has the same suit as the hidden card!

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 20, 2007.

lec 10F.24

4	9	13	7
12	10	6	1
3	11	8	14
15	5	16	2

Magic Trick Revealed (II)

How does Jessica figure out the value of the hidden card?

Aha! Look at the order of the other 3 cards!

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 20, 2007.

lec 10F.25

4	9	13	7
12	10	6	1
3	11	8	14
15	5	16	2

Magic Trick Revealed (II)

Fix ordering of the deck

$A\clubsuit < 2\clubsuit < 3\clubsuit < \dots < K\clubsuit <$

$A\diamondsuit < 2\diamondsuit < 3\diamondsuit < \dots < K\diamondsuit <$

$A\heartsuit < 2\heartsuit < 3\heartsuit < \dots < K\heartsuit <$

$A\spadesuit < 2\spadesuit < 3\spadesuit < \dots < K\spadesuit$

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 20, 2007.

lec 10F.26

4	9	13	7
12	10	6	1
3	11	8	14
15	5	16	2

Magic Trick Revealed (II)

Possible orders for the remaining 3 cards:

{ **SML, SLM, MSL, MLS, LSM, LMS** }

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 20, 2007.

lec 10F.27

4	9	13	7
12	10	6	1
3	11	8	14
15	5	16	2

Magic Trick Revealed (II)

Wait! Only have 6 lists of the remaining 3 cards, but 12 possible hidden cards of the known suit!

Of two cards with the same suit, choosing which to reveal can give 1 more bit of information!
Aha!

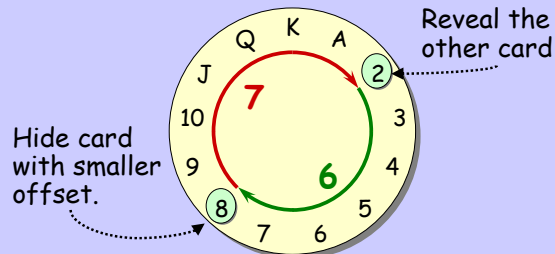
Copyright © 2007 by Albert R. Meyer. All rights reserved. April 20, 2007.

lec 10F.28

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

Clockwise Distance

The *smaller clockwise distance* between 2 card values is at most **6**:



Copyright © 2007 by Albert R. Meyer. All rights reserved. April 20, 2007.

lec 10F.29

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

Magic Trick Revealed (Finally)

- The first card determines the hidden suit ($\spadesuit \heartsuit \diamondsuit \clubsuit$).
- Hidden value (A ... K) = first-card value + offset (≤ 6).
- Offset given by order of remaining 3 cards:
 $SML = 1, SLM = 2, MSL = 3,$
 $MLS = 4, LSM = 5, LMS = 6.$

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 20, 2007.

lec 10F.30

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

Example

First: Hidden:

Offset = 1 = **SML**:

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 20, 2007.

lec 10F.31

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

Trick can't work with 4-card hands

Students can pick

$$\binom{52}{4} = 270,725$$

possible 4-card hands

Chiyoun can reveal

$$\frac{52!}{49!} = 132,600$$

possible 3-card lists

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 20, 2007.

lec 10F.32

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

Trick can't work with 4 cards hands so at least

$$\left\lceil \frac{270,225}{132,600} \right\rceil = 3$$

hands map to the **same list**
- Jessica can't tell which!

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 20, 2007.

lec 10F.33

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

Team Problems

Problem 1
(& 2 & 3)

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 20, 2007.

lec 10F.35

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

Binomial Theorem, Combinatorial Proof

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 23, 2006.

lec 11M.2

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

Polynomials Express Choices & Outcomes

$$(\text{red tie} + \text{orange tie} + \text{yellow tie}) (\text{orange tie} + \text{gray tie}) =$$

$$\text{red tie orange tie} + \text{red tie gray tie} + \text{orange tie orange tie} + \text{orange tie gray tie} + \text{yellow tie orange tie} + \text{yellow tie gray tie}$$

Products of Sum = Sums of Products

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 23, 2006.

lec 11M.3

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

Expression for c_k ?

$$(1+X)^n =$$

$$c_0 + c_1X + c_2X^2 + \dots + c_nX^n$$

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 23, 2006.

lec 11M.4

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

Expression for c_k ?

$$(1+X)^n \quad \text{n times}$$

$$= (1+X)(1+X)(1+X)(1+X)\dots(1+X)$$

multiplying gives 2^n product terms:
 $11\dots 1 + X11\dots 1 + 1X11\dots 1 + \dots + XX\dots X$
 a term corresponds to selecting 1 or X from each of the n factors.

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 23, 2006.

lec 11M.5

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

Expression for c_k ?

$$(1+X)^n \quad \text{n times}$$

$$= (1+X)(1+X)(1+X)(1+X)\dots(1+X)$$

the X^k coeff, c_k , is number of terms where exactly k X's were selected.

$$c_k = \binom{n}{k}$$

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 23, 2006.

lec 11M.6

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

The Binomial Formula

$$(1+X)^n =$$

$$\binom{n}{0} + \binom{n}{1}X + \binom{n}{2}X^2 + \dots + \binom{n}{k}X^k + \dots + \binom{n}{n}X^n$$

binomial expression

binomial coefficients

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 23, 2006.

lec 11M.7

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

The Binomial Formula

$$\begin{aligned}
 (1+X)^0 &= 1 \\
 (1+X)^1 &= 1 + 1X \\
 (1+X)^2 &= 1 + 2X + 1X^2 \\
 (1+X)^3 &= 1 + 3X + 3X^2 + 1X^3 \\
 (1+X)^4 &= 1 + 4X + 6X^2 + 4X^3 + 1X^4
 \end{aligned}$$

Copyright ©2007 by Albert R. Meyer. All rights reserved. April 23, 2006.

lec 11M.8

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

The Binomial Formula

$$\begin{aligned}
 (X + Y)^n &= \\
 &\binom{n}{0}Y^n + \binom{n}{1}XY^{n-1} + \binom{n}{2}X^2Y^{n-2} + \\
 &\dots + \binom{n}{k}X^kY^{n-k} + \dots + \binom{n}{n}X^n
 \end{aligned}$$

Copyright ©2007 by Albert R. Meyer. All rights reserved. April 23, 2006.

lec 11M.9

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

The Binomial Formula

$$(X + Y)^n = \sum_{k=0}^n \binom{n}{k} X^k Y^{n-k}$$

Copyright ©2007 by Albert R. Meyer. All rights reserved. April 23, 2006.

lec 11M.10

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

Multinomials

What is the coefficient of
EMSTY
in the expansion of
(E + M + S + T + Y)⁵ ?

5!

Copyright ©2007 by Albert R. Meyer. All rights reserved. April 23, 2006.

lec 11M.11

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

Multinomials

What is the coefficient of
EMS³TY
in the expansion of
(E + M + S + T + Y)⁷ ?

The number of ways to
rearrange the letters in
the word
SYSTEMS

Copyright ©2007 by Albert R. Meyer. All rights reserved. April 23, 2006.

lec 11M.12

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

Applying the BOOKKEEPER rule

What is the coefficient of
EMS³TY
in the expansion of
(E + M + S + T + Y)⁷ ?

7!
1! 1! 3! 1! 1!

Copyright ©2007 by Albert R. Meyer. All rights reserved. April 23, 2006.

lec 11M.13

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

Multinomial Coefficients

$$\binom{7}{1,1,3,1,1} ::= \frac{7!}{1! 1! 3! 1! 1!}$$

Copyright ©2007 by Albert R. Meyer. All rights reserved. April 23, 2006.

lec 11M.14

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

Multinomial Coefficients

$$\binom{n}{r_1, r_2, \dots, r_k} ::= \frac{n!}{r_1! r_2! \dots r_k!}$$

$$= 0 \quad \text{if } r_1 + r_2 + \dots + r_k \neq n$$

Copyright ©2007 by Albert R. Meyer. All rights reserved. April 23, 2006.

lec 11M.15

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

Multinomial Coefficients

What is the coefficient of BA^3N^2
in the expansion of
 $(B + A + N)^6$?

The number of ways to
rearrange the letters in
the word
BANANA

Copyright ©2007 by Albert R. Meyer. All rights reserved. April 23, 2006.

lec 11M.16

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

Multinomial Coefficients

What is the coefficient of BA^3N^2
in the expansion of
 $(B + A + N)^6$?

$$\binom{6}{1,3,2}$$

Copyright ©2007 by Albert R. Meyer. All rights reserved. April 23, 2006.

lec 11M.17

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

Multinomial Coefficients

What is the coefficient of
 $X_1^{r_1} X_2^{r_2} X_3^{r_3} \dots X_k^{r_k}$
in the expansion of
 $(X_1 + X_2 + X_3 + \dots + X_k)^n$?

$$\binom{n}{r_1, r_2, r_3, \dots, r_k}$$

Copyright ©2007 by Albert R. Meyer. All rights reserved. April 23, 2006.

lec 11M.18

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

Multinomial Coefficients

Binomial a special case:

$$\binom{n}{k} = \binom{n}{k, n-k}$$

Copyright ©2007 by Albert R. Meyer. All rights reserved. April 23, 2006.

lec 11M.19

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

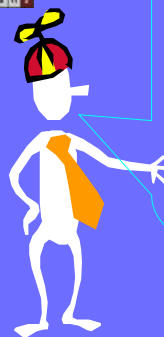
The Multinomial Formula

$$(X_1 + X_2 + \dots + X_k)^n = \sum_{\substack{r_1, r_2, \dots, r_k \\ \sum r_i = n}} \binom{n}{r_1, r_2, \dots, r_k} X_1^{r_1} X_2^{r_2} X_3^{r_3} \dots X_k^{r_k}$$

Copyright ©2007 by Albert R. Meyer. All rights reserved. April 23, 2006.

lec 11M.20

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



More next week about how polynomials encode counting questions!

Copyright ©2007 by Albert R. Meyer. All rights reserved. April 23, 2006.

lec 11M.21

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

Pascal's Identity

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

Algebraic Proof: routine, using

$$\binom{n}{k} ::= \frac{n!}{k!(n-k)!} = \frac{n(n-1)!}{k(k-1)!(n-k)!} = \frac{n}{k} \binom{n-1}{k-1}$$

Copyright ©2007 by Albert R. Meyer. All rights reserved. April 23, 2006.

lec 11M.23

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

Combinatorial Proof

Consider subsets of $\{1, \dots, n\}$

size k subsets =
 # size k subsets that **contain a 1**
 + # size k subsets that **do not contain a 1**

Copyright ©2007 by Albert R. Meyer. All rights reserved. April 23, 2006.

lec 11M.24

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

Combinatorial Proof

Consider subsets of $\{1, \dots, n\}$

$$\underbrace{\binom{n}{k}}_{\substack{\text{\# size } k \\ \text{subsets}}} = \underbrace{\binom{n-1}{k}}_{\substack{\text{\# size } k \\ \text{subsets}}} + \underbrace{\binom{n-1}{k-1}}_{\substack{\text{\# size } k-1 \\ \text{subsets}}}$$

Copyright ©2007 by Albert R. Meyer. All rights reserved. April 23, 2006.

lec 11M.25

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

Combinatorial Proof

Consider subsets of $\{1, \dots, n\}$

$$\underbrace{\binom{n}{k}}_{\substack{\text{\# size } k \\ \text{subsets}}} = \underbrace{\binom{n-1}{k}}_{\substack{\text{\# size } k \\ \text{subsets}}} + \underbrace{\binom{n-1}{k-1}}_{\substack{\text{\# size } k-1 \\ \text{subsets:} \\ \text{with no } 1}}$$

Copyright ©2007 by Albert R. Meyer. All rights reserved. April 23, 2006.

lec 11M.26

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

Combinatorial Proof

Consider subsets of $\{1, \dots, n\}$

$$\underbrace{\binom{n}{k}}_{\substack{\text{\# size } k \\ \text{subsets}}} = \underbrace{\binom{n-1}{k}}_{\substack{\text{\# size } k \\ \text{subsets:} \\ \text{with no } 1}} + \underbrace{\binom{n-1}{k-1}}_{\substack{\text{\# size } k \\ \text{subsets:} \\ \text{with a } 1}}$$

Copyright ©2007 by Albert R. Meyer. All rights reserved. April 23, 2006.

lec 11M.27

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

Combinatorial Proof

$$\sum_{i=0}^n \binom{n}{i}^2 = \binom{2n}{n}$$

Copyright ©2007 by Albert R. Meyer. All rights reserved. April 23, 2006.

lec 11M.28

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

Combinatorial Proof

Consider subsets of $\{1, \dots, n, 1, \dots, n\}$

$$\sum_{i=0}^n \binom{n}{i}^2 = \underbrace{\binom{2n}{n}}_{\substack{\text{\# size } n \\ \text{subsets}}}$$

Copyright ©2007 by Albert R. Meyer. All rights reserved. April 23, 2006.

lec 11M.29

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

Combinatorial Proof

$$\begin{aligned} \text{LHS} &= \sum_{i=0}^n \binom{n}{i}^2 \\ &= \sum_{i=0}^n \binom{n}{i} \binom{n}{n-i} \end{aligned}$$

Copyright ©2007 by Albert R. Meyer. All rights reserved. April 23, 2006.

lec 11M.30

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

Combinatorial Proof

LHS =

$$\sum_{i=0}^n \underbrace{\binom{n}{i}}_{\substack{\text{\# size } i \\ \text{red subsets}}} \binom{n}{n-i}$$

Copyright ©2007 by Albert R. Meyer. All rights reserved. April 23, 2006.

lec 11M.31

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

Combinatorial Proof

LHS =

$$\sum_{i=0}^n \underbrace{\binom{n}{i}}_{\substack{\text{\# size } i \\ \text{red subsets}}} \underbrace{\binom{n}{n-i}}_{\substack{\text{\# size } n-i \\ \text{black subsets}}}$$

Copyright ©2007 by Albert R. Meyer. All rights reserved. April 23, 2006.

lec 11M.32

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

Combinatorial Proof

$$\sum_{i=0}^n \underbrace{\binom{n}{i}}_{\substack{\text{\# size } i \\ \text{red subsets}}} \underbrace{\binom{n}{n-i}}_{\substack{\text{\# size } n-i \\ \text{black subsets}}}$$

So LHS = # size n subsets
of $\{1, \dots, n, 1, \dots, n\}$
by the Sum Rule

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 23, 2006.

lec 11M.33

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

Combinatorial Proof

Therefore
LHS = # size n subsets = RHS

$$\sum_{i=0}^n \binom{n}{i}^2 = \binom{2n}{n}$$

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 23, 2006.

lec 11M.34

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

Team Problems

Problems
1–4

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 23, 2006.

lec 11M.35

(Video Cam notes, copyright Albert R. Meyer 2007)

Generating Functions for

 k Counting

$$(1+q_1)(1+q_2)\dots(1+q_k) = \sum_{i=0}^k \binom{k}{i} x^i$$

$$2^k \left\{ \begin{array}{l} | | | \cdot | + \\ x | | | | | + \\ | x | | | | + \\ \vdots \\ x \dots x + \end{array} \right.$$

How many ways to select of
sequence, n , of pennies & nickels that
 sum to k ¢ n

$$(x + x^5)(x + x^5) \dots (x + x^5)$$

answer is # terms of degree k

choose nickel, nickel, penny, penny, nickel

$$x^5 \quad x^5 \quad x \quad x \quad x^5 = x^{17}$$

coefficient of x^k in

$$(x + x^5)^n$$

k kinds of donuts, want to buy n donuts,
how many such selections?

$$\binom{n + (k-1)}{k-1}$$

chocolate $1 + 1 \cdot c + 1 \cdot c^2 + 1 \cdot c^3 + \dots$

vanilla $1 + 1 \cdot v + 1 \cdot v^2 + 1 \cdot v^3 + \dots$

k^{th} -kind $1 + 1 \cdot d + 1 \cdot d^2 + \dots$

answer is the ~~coefficient~~ of
number of degree n
terms in

$$\left. \begin{aligned} &(1 + c + c^2 + \dots)(1 + v + v^2 + \dots) \dots (1 + d + d^2 + \dots) \\ &(1 + x + x^2 + \dots)(1 + x + x^2 + \dots) \dots (1 + x + x^2 + \dots) \end{aligned} \right\}$$

coeff of x^n is # ways of selecting
 n donuts among k kinds

coeff. of x^n in

$$(1+x+x^2+\dots)^k = \left(\frac{1}{1-x}\right)^k$$

is

$$\binom{n+k-1}{k-1} = \frac{1}{(1-x)^k}$$

Taylor series

$$F(x) = f_0 + f_1 x + f_2 x^2 + f_3 x^3 + \dots$$

$$f_0 = F(0)$$

$$F'(x) = f_1 + 2f_2 x + 3f_3 x^2 + \dots$$

$$f_1 = F'(0)$$

$$F''(x) = 2f_2 + 3 \cdot 2 f_3 x + 4 \cdot 3 f_4 x^2 + \dots$$

$$f_2 = \frac{F^{(2)}(0)}{2!}$$

$$f_n = \frac{F^{(n)}(0)}{n!}$$

$$A(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \dots + a_nx^n$$

$$B(x) = b_0 + b_1x + \dots + b_nx^n$$

Convolution's Counting Principle
 $C(x) = A(x)B(x)$ coefficient of x^n

tells me the # ways to
 form a mixed collection of
 a's & b's that totals to n

$$C_n = \underbrace{b_0a_n + b_1a_{n-1} + b_2a_{n-2} + \dots + b_na_0}_{\text{convolution}}$$

Counting baskets of n fruits
in a basket must have

≤ 2 Bananas

$$B(x) = 1 + x + x^2 = \frac{1-x^3}{1-x}$$

≤ 4 Pears

$$P(x) = 1 + x + x^2 + x^3 + x^4 = \frac{1-x^5}{1-x}$$

even # apples

$$A(x) = 1 + 0x + 1x^2 + 0x^3 + 1x^4 + \dots = (1 + x^2 + x^4 + x^6 + \dots) = \frac{1}{1-x^2}$$

oranges is
divisible by 5

$$O(x) = (1 + x^5 + x^{10} + \dots) = \frac{1}{1-x^5}$$

baskets of n fruit is coefficient of x^n

$$\text{in } F(x) = B(x) \cdot P(x) \cdot A(x) \cdot O(x)$$

$$= \frac{1-x^3}{1-x} \cdot \frac{1-x^5}{1-x} \cdot \frac{1}{1-x^2} \cdot \frac{1}{1-x^5}$$

$$= \frac{1-x^3}{(1-x)^3 \cdot (1+x)}$$

$$f(x) = \frac{1-x^3}{(1-x)^3(1+x)}$$

$$\Rightarrow \frac{a}{1-x} + \frac{b}{(1-x)^2} + \frac{c}{(1-x)^3} + \frac{d}{1+x}$$

$$1-x^3 \Rightarrow a(1-x)^2(1+x) + b(1-x)(1+x) + c(1+x) + d(1-x)^3$$

$$\text{let } x=-1 : 2 = d \cdot 2^3 \Rightarrow d = \frac{1}{4}$$

$$x=1 : 0 = c \cdot 2 \Rightarrow c=0$$

$$x=0 : a+b+c+d=1 \Rightarrow a+b = \frac{3}{4}$$

$$x=\frac{1}{2} : \Rightarrow b = \frac{3}{2}, a = -\frac{3}{4}$$

$$\text{Coeff of } x^n : a + b \binom{n+2+1}{2-1} + c(-1) + d(-1)^n$$

$$= -\frac{3}{4} + \frac{3}{2} \binom{n+1}{1} + \frac{1}{4}(-1)^n$$

$$n=1?$$

$$= \frac{6(n+1) - 3 + (-1)^n}{4}$$

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

Generating Functions for Recurrences

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 27, 2007.

lec 11F.1

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

The Rabbit Population



- A mature boy/girl rabbit pair reproduces every month.
- Rabbits mature after one month.

$w_n ::=$ # newborn pairs after n months

$r_n ::=$ # reproducing pairs after n months

- Start with a newborn pair: $w_0 = 1$
 $r_0 = 0$

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 27, 2007.

lec 11F.2

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

The Rabbit Population



$w_n ::=$ # newborn pairs after n months

$r_n ::=$ # reproducing pairs after n months

$$r_1 = 1$$

$$r_n = r_{n-1} + w_{n-1}$$

$$w_n = r_{n-1} \text{ so}$$

$$r_n = r_{n-1} + r_{n-2}$$

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 27, 2007.

lec 11F.3

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

The Rabbit Population



$$r_n = r_{n-1} + r_{n-2}$$

It was Fibonacci who was studying rabbit population growth

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 27, 2007.

lec 11F.4

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

Generating Function for Rabbits

$$R(x) ::= r_0 + r_1x + r_2x^2 + r_3x^3 + \dots$$

$$-xR(x) = -r_0x - r_1x^2 - r_2x^3 - \dots$$

$$-x^2R(x) = -r_0x^2 - r_1x^3 - \dots$$

0

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 27, 2007.

lec 11F.5

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

Generating Function for Rabbits

$$R(x) ::= r_0 + r_1x + r_2x^2 + r_3x^3 + \dots$$

$$-xR(x) = -r_0x - r_1x^2 - r_2x^3 - \dots$$

$$-x^2R(x) = -r_0x^2 - r_1x^3 - \dots$$

0

0

...

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 27, 2007.

lec 11F.6

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

Generating Function for Rabbits

$$R(x) ::= r_0 + r_1 x$$

$$-xR(x) = -r_0 x$$

$$-x^2 R(x) =$$

$$R(x) - xR(x) - x^2 R(x) = r_0 + r_1 x - r_0 x = x$$

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 27, 2007.

lec 11F.7

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

Generating Function for Rabbits

$$R(x) = \frac{x}{1 - x - x^2}$$

Now find closed form for r_n :

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 27, 2007.

lec 11F.8

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

Closed Form for r_n

$$R(x) = \frac{x}{1 - x - x^2}$$

$$= \frac{x}{(1 - \alpha x)(1 - \beta x)}$$

α, β are 1/roots of $1 - x - x^2$

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 27, 2007.

lec 11F.9

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

Closed Form for r_n

$$R(x) = \frac{x}{(1 - \alpha x)(1 - \beta x)}$$

$$= \frac{a}{1 - \alpha x} + \frac{b}{1 - \beta x}$$

so

$$r_n = a\alpha^n + b\beta^n$$

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 27, 2007.

lec 11F.10

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

Closed Form for r_n from quadratic formula:

$$\alpha = \frac{1 + \sqrt{5}}{2}$$

$$\beta = \frac{1 - \sqrt{5}}{2}$$

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 27, 2007.

lec 11F.11

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

Closed Form for r_n

$$x = a(1 - \beta x) + b(1 - \alpha x)$$

$$x=1/\beta: \quad 1/\beta = b(1 - \alpha/\beta)$$

$$b = 1/(\beta - \alpha)$$

$$\text{likewise} \quad a = 1/(\alpha - \beta)$$

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 27, 2007.

lec 11F.12

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

Closed Form for r_n

$$r_n = a\alpha^n + b\beta^n$$

$$= \frac{1}{\sqrt{5}} \left(\frac{1 + \sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left(\frac{1 - \sqrt{5}}{2} \right)^n$$

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 27, 2007.

lec 11F.13

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

Closed Form for r_n

$$r_n = \left\lfloor \frac{((1 + \sqrt{5})/2)^n}{\sqrt{5}} \right\rfloor$$

$$(1.61)^n = o(r_n)$$

$$r_n = o((1.62)^n)$$

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 27, 2007.

lec 11F.14

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

Towers of Hanoi



$\text{Move}_{1,2}(n) ::= \text{Move}_{1,3}(n-1);$
big disk $1 \rightarrow 2;$
 $\text{Move}_{3,2}(n-1)$

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 27, 2007.

lec 11F.15

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

Towers of Hanoi

$s_n ::= \# \text{ steps by } \text{Move}_{1,2}(n)$

$$s_n = 2s_{n-1} + 1$$

$$s_0 = 0$$

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 27, 2007.

lec 11F.16

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

Hanoi Generating Function

$$S(x) ::= s_0 + s_1x + s_2x^2 + s_3x^3 + \dots$$

$$-2xS(x) = -2s_0x - 2s_1x^2 - 2s_2x^3 - \dots$$

$$-x/(1-x) = -1 \cdot x^1 - 1 \cdot x^2 - 1 \cdot x^3 - \dots$$

0 0 0 ...

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 27, 2007.

lec 11F.17

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

Hanoi Generating Function

$$S(x) = s_0 = 0$$

$$-2xS(x)$$

$$-x/(1-x)$$

$$S(x) = \frac{x}{(1-x)(1-2x)}$$

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 27, 2007.

lec 11F.18

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Hanoi Generating Function

$$S(x) = \frac{x}{(1-x)(1-2x)}$$

$$= \frac{a}{1-x} + \frac{b}{1-2x}$$

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 27, 2007.

lec 11F.19

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Hanoi Generating Function

$$x = a(1-2x) + b(1-x)$$

for $x = 1$: $1 = a(-1)$, so

$$a = -1$$

$x = 1/2$: $1/2 = b(1/2)$, so

$$b = 1$$

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 27, 2007.

lec 11F.20

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Hanoi Generating Function

$$S(x) = \frac{1}{1-2x} - \frac{1}{1-x}$$

$$\text{so } s_n = 2^n - 1$$

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 27, 2007.

lec 11F.21

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Team Problems

Problems

1 & 2

Copyright © 2007 by Albert R. Meyer. All rights reserved. April 27, 2007.

lec 11F.22

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

Introduction to Probability Theory

Copyright © 2007, Albert R. Meyer. All rights reserved.

April 30, 2007

lec 12M.1

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

Counting in Probability

What is the probability of getting exactly two jacks in a poker hand?



Copyright © 2007, Albert R. Meyer. All rights reserved.

April 30, 2007

lec 12M.2

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

Counting in Probability

Outcomes: $\binom{52}{5}$ 5-card hands



Event: $\binom{4}{2} \cdot \binom{52-4}{3}$ hands w/2Jacks.

$$\Pr\{2J\} ::= \frac{\binom{4}{2} \cdot \binom{48}{3}}{\binom{52}{5}} \approx 0.04$$

Copyright © 2007, Albert R. Meyer. All rights reserved.

April 30, 2007

lec 12M.3

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

Probability: 1st Idea

- set of basic experimental outcomes,
- subset of outcomes considered a noteworthy event,
- probability{event}

$$::= \frac{\# \text{ outcomes in event}}{\# \text{ possible outcomes}}$$

Copyright © 2007, Albert R. Meyer. All rights reserved.

April 30, 2007

lec 12M.4

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

The Monty Hall Game

Applied Probability:
Let's Make A Deal
(1970's TV Game Show)

Copyright © 2007, Albert R. Meyer. All rights reserved.

April 30, 2007

lec 12M.5

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

Monty Hall Webpages



<http://www.letsmakeadeal.com>

Copyright © 2007, Albert R. Meyer. All rights reserved.

April 30, 2007

lec 12M.6

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Analyzing Monty Hall

Marilyn Vos Savant explained Game in magazine -- bombarded by letters (even from PhD's) debating:

- 1) sticking & switching equally good
- 2) switching better

Copyright © 2007, Albert R. Meyer. All rights reserved.

April 30, 2007

lec 12M.9

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Analyzing Monty Hall

Determine the outcomes.
-- a tree of possible steps can help

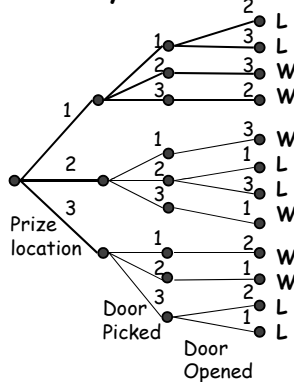
Copyright © 2007, Albert R. Meyer. All rights reserved.

April 30, 2007

lec 12M.10

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Monty Hall SWITCH Strategy



SWITCH
Wins: 6
Lose: 6

Copyright © 2007, Albert R. Meyer. All rights reserved.

April 30, 2007

lec 12M.11

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Monty Hall STICK Strategy

Win by sticking
iff
Lose by switching.

STICK
Lose: 6
Wins: 6

Copyright © 2007, Albert R. Meyer. All rights reserved.

April 30, 2007

lec 12M.12

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Analyzing Monty Hall

Sticking and Switching have same # winning outcomes.

False conclusion:
Contestant has same probability of winning:

$\frac{1}{2}$

Copyright © 2007, Albert R. Meyer. All rights reserved.

April 30, 2007

lec 12M.13

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

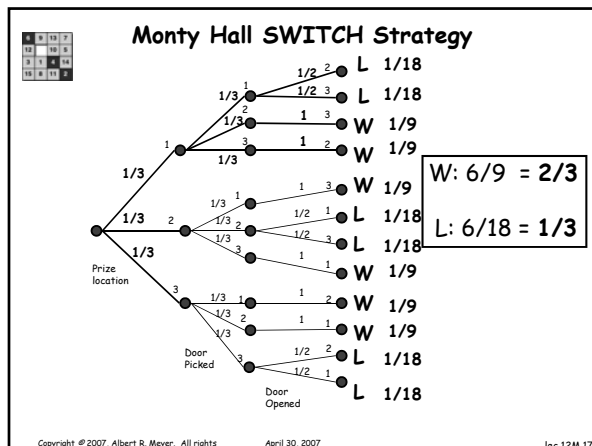
Analyzing Monty Hall

What's wrong?
Let's look at the outcome tree more carefully.

Copyright © 2007, Albert R. Meyer. All rights reserved.

April 30, 2007

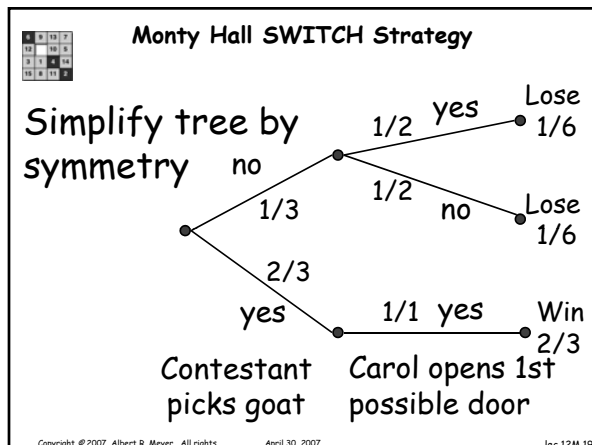
lec 12M.16



Probability: 2nd Idea

Outcomes may have differing probabilities!
Not always uniform.

Copyright © 2007, Albert R. Meyer. All rights reserved. April 30, 2007 lec 12M.18



Finding Probability

Intuition is important but dangerous.
Stick with 4-part method:

1. Identify outcomes (*tree helps*)
2. Identify event (*winning*)
3. Assign outcome probabilities
4. Compute event probabilities

Copyright © 2007, Albert R. Meyer. All rights reserved. April 30, 2007 lec 12M.21

Probability Spaces

- 1) Sample space, \mathcal{S} , whose elements are called outcomes.
- 2) Probability function, $\Pr: \mathcal{P}(\mathcal{S}) \rightarrow [0,1]$
 - (a) $\Pr\{\mathcal{S}\} = 1$,
 - (b) the Sum Rule:

Copyright © 2007, Albert R. Meyer. All rights reserved. April 30, 2007 lec 12M.22

(Disjoint) Sum Rule

If A_1, A_2 are disjoint,

$$\Pr\{A_1 \cup A_2\} = \Pr\{A_1\} + \Pr\{A_2\}$$

Copyright © 2007, Albert R. Meyer. All rights reserved. April 30, 2007 lec 12M.23

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

Sum Rule (Infinite)

For pairwise disjoint A_0, A_1, \dots

$$\Pr\{A_0 \cup A_1 \cup \dots\} = \Pr\{A_0\} + \Pr\{A_1\} + \dots$$

Copyright © 2007, Albert R. Meyer. All rights

April 30, 2007

lec 12M.24

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

Inclusion-Exclusion

$$\begin{aligned} \Pr\{A \cup B\} \\ &= \Pr\{A\} + \Pr\{B\} \\ &\quad - \Pr\{A \cap B\} \end{aligned}$$

Copyright © 2007, Albert R. Meyer. All rights

April 30, 2007

lec 12M.27

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

The Union Bound

$$\begin{aligned} \Pr\{A \cup B\} \\ \leq \Pr\{A\} + \Pr\{B\} \end{aligned}$$

Copyright © 2007, Albert R. Meyer. All rights

April 30, 2007

lec 12M.28

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

Team Problems

Problems

1–4

Copyright © 2007, Albert R. Meyer. All rights

April 30, 2007

lec 12M.31

6	9	13	7
12	10	5	
3	4	8	14
15	11	16	2

Conditional Probability & Independence

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 2, 2007

lec 12W.1

6	9	13	7
12	10	5	
3	4	8	14
15	11	16	2

Conditional Probability: Dice

$$\Pr\{\text{die rolled } 1\} = 1/|\{1,2,3,4,5,6\}| = 1/6.$$

"Knowledge" changes probabilities:

$$\begin{aligned} \Pr\{\text{die rolled } 1 \text{ knowing} \\ \text{that die rolled odd number}\} \\ &= 1/|\{1,3,5\}| \\ &= 1/3. \end{aligned}$$

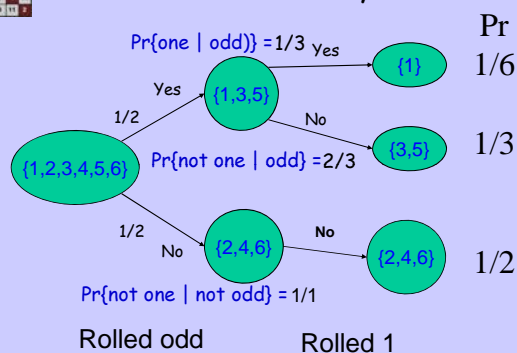
Copyright © 2007, Albert R. Meyer. All rights reserved.

May 2, 2007

lec 12W.2

6	9	13	7
12	10	5	
3	4	8	14
15	11	16	2

Conditional Probability: Dice



Copyright © 2007, Albert R. Meyer. All rights reserved.

May 2, 2007

lec 12W.3

6	9	13	7
12	10	5	
3	4	8	14
15	11	16	2

Conditional Probability

$\Pr\{A \mid B\}$ is the prob.
of event A , **given** that
event B has occurred

$$\Pr\{A \mid B\} ::= \frac{\Pr\{A \cap B\}}{\Pr\{B\}}$$

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 2, 2007

lec 12W.4

6	9	13	7
12	10	5	
3	4	8	14
15	11	16	2

Product Rule

$$\Pr\{A \cap B\} = \Pr\{A \mid B\} \Pr\{B\}$$

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 2, 2007

lec 12W.5

6	9	13	7
12	10	5	
3	4	8	14
15	11	16	2

Conditional Probability: Monty Hall

$$\Pr\{\text{prize at } 1 \mid \text{Goat at } 2\} = 1/2$$

Really!

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 2, 2007

lec 12W.6

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Conditional Probability: Monty Hall

$$\Pr\{\text{prize at 1} \mid \text{Goat at 2}\} = 1/2$$

Outcomes: Really!

(Prize Door, Picked Door, Carol door)

[Goat at 2] =

$\{(1,1,2), (1,1,3), (1,2,3), (1,3,2),$
 $(3,3,1), (3,3,2), (3,1,2), (3,2,1)\}$

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 2, 2007

lec 12W.7

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Conditional Probability: Monty Hall

$$\Pr\{\text{prize at 1} \mid \text{Goat at 2}\} = 1/2$$

Really! Outcomes:

(Prize Door, Picked Door, Carol door)

[Goat at 2] =

$\{(1,1,2), (1,1,3), (1,2,3), (1,3,2),$
 $(3,3,1), (3,3,2), (3,1,2), (3,2,1)\}$

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 2, 2007

lec 12W.8

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Conditional Probability: Monty Hall

$$\Pr\{\text{prize at 1} \mid \text{Carol opens 2}\} = 1/2$$

Outcomes:

(Prize Door, Picked Door, Carol door)

[Carol opens 2] =

$\{(1,1,2), (1,3,2),$
 $(3,3,2), (3,1,2)\}$

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 2, 2007

lec 12W.9

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Conditional Probability: Monty Hall

$$\Pr\{\text{prize at 1} \mid \text{Carol opens 2}\} = 1/2$$

Outcomes:

(Prize Door, Picked Door, Carol door)

[Carol opens 2] =

$\{(1,1,2), (1,3,2),$
 $(3,3,2), (3,1,2)\}$

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 2, 2007

lec 12W.10

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Conditional Probability: Monty Hall

This suggests the contestant may as well stick, since the probability is 1/2 *given what he knows* when he chooses. But wait: contestant **knows more** than door opened by Carol -- also knows: **which door he chose** himself!

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 2, 2007

lec 12W.11

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Conditional Probability: Monty Hall

$$\Pr\{\text{prize at 1} \mid \text{picked 1 \& Carol opens 2}\} = 1/3$$

[picked 1 & Carol opens 2] =

$\{(1,1,2), (3,1,2)\}$

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 2, 2007

lec 12W.12

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Conditional Probability: Monty Hall

$$\Pr\{\text{prize at 1} \mid \text{picked 1 \& Carol opens 2}\} = 1/3$$

$$[\text{picked 1 \& Carol opens 2}] = \{(1,1,2), (3,1,2)\}$$

$$\Pr=1/18 \quad \Pr=1/9$$

$$\frac{1/18}{1/18+1/9} = \frac{1}{3}$$

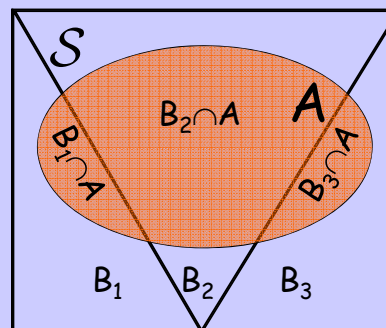
Copyright © 2007, Albert R. Meyer. All rights reserved.

May 2, 2007

lec.12W.13

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Law of Total Probability



Copyright © 2007, Albert R. Meyer. All rights reserved.

May 2, 2007

lec.12W.14

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Law of Total Probability

$$A = (B_1 \cap A) \cup (B_2 \cap A) \cup (B_3 \cap A)$$

$$\Pr\{A\} = \Pr\{B_1 \cap A\} + \Pr\{B_2 \cap A\} + \Pr\{B_3 \cap A\}$$

$$= \Pr\{A|B_1\} \cdot \Pr\{B_1\} + \Pr\{A|B_2\} \cdot \Pr\{B_2\} + \Pr\{A|B_3\} \cdot \Pr\{B_3\}$$

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 2, 2007

lec.12W.15

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Team Problems

Problems 1 & 2

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 2, 2007

lec.12W.17

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Definitions of Independence

Definition 1:

Events A and B are independent iff

$$\Pr\{A\} = \Pr\{A \mid B\}.$$

Definition 2:

Events A and B are independent iff

$$\Pr\{A\} \cdot \Pr\{B\} = \Pr\{A \cap B\}.$$

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 2, 2007

lec.12W.19

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Definitions of Independence

Equivalent:

$$\Pr\{A\} = \Pr\{A \mid B\} \quad \text{iff}$$

$$\Pr\{A\} = \frac{\Pr\{A \cap B\}}{\Pr\{B\}} \quad \text{iff}$$

$$\Pr\{A\} \cdot \Pr\{B\} = \Pr\{A \cap B\}.$$

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 2, 2007

lec.12W.20

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

Definitions of Independence

Note: need $\Pr\{B\} \neq 0$ for Def. 1.

Def. 2 works even if 0:

$$\Pr\{A\} \cdot \Pr\{B\} = \Pr\{A \cap B\}$$

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 2, 2007

lec 12W.21

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

The Birthday "Paradox"

Puzzle: n students in a room.
Probability that two have the
same birthday (month, day)
for $n = 2, 10, 23, 30, 107$?

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 2, 2007

lec 12W.22

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

The Birthday "Paradox"

- So with 10 students have
 $10/365 \approx 1/30$ chance 2 have
same b'day?
Not really, it's more like 1/10.
- With 30 students, maybe
 $3 \cdot (30/365) \approx 1/3$ chance?
No, it's more than 2 to 1!

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 2, 2007

lec 12W.23

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

The Birthday "Paradox"

Let's stop guessing and figure it
out. Let's assume 6.042
students are *equally likely* to
have each of 365 possible
birthdays.

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 2, 2007

lec 12W.24

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

The Birthday "Paradox"

Choose 2 students at random.
 $\Pr\{2 \text{ students have same b'day}\}$

$$= \frac{1}{365}$$

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 2, 2007

lec 12W.25

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

The Birthday "Paradox"

$\Pr\{2 \text{ students b'days differ}\}$

$$= 1 - \frac{1}{365}$$

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 2, 2007

lec 12W.26

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

The Birthday "Paradox"

Choose **another** 2 students
independently of first two.
 $\Pr\{\text{neither pair has same birthday}\}$
 $= \Pr\{\text{1st pair's b'days differ and}$
 **2nd pair's b'days differ}\}
 $= \Pr\{\text{1st pair's b'days differ}\} \times$
 $\Pr\{\text{2nd pair's b'days differ}\}$**

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 2, 2007

lec 12W.31

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

The Birthday "Paradox"

$$\Pr\{\text{both pairs' b'days differ}\}$$

$$= \left(1 - \frac{1}{365}\right)^2$$

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 2, 2007

lec 12W.32

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

The Birthday "Paradox"

Choose another **253** pairs of students
independently of first pairs.
 $\Pr\{\text{no pair has same birthday}\}$

$$= \left(1 - \frac{1}{365}\right)^{253} \approx \frac{1}{2}$$

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 2, 2007

lec 12W.33

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

The Birthday "Paradox"

But with $n = 23$ students,
 have $\binom{23}{2} = 253$ pairs
 of students.

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 2, 2007

lec 12W.34

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

The Birthday "Paradox"

So, with **23** students
 $\Pr\{\text{no pair has same b'day}\}$

$$\approx \frac{1}{2}$$

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 2, 2007

lec 12W.35

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

The Birthday "Paradox"

With **140** students
 $\Pr\{\text{no pair has same b'day}\}$

$$\approx \left(1 - \frac{1}{365}\right)^{\binom{140}{2}} = \left(1 - \frac{1}{365}\right)^{9730}$$

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 2, 2007

lec 12W.36

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

The Birthday "Paradox"

With 140 students

$\Pr\{\text{no pair has same b'day}\}$

$$= \left(1 - \frac{1}{365}\right)^{365 \binom{140}{2}} \leq e^{-\frac{1}{365} \binom{140}{2}}$$

$$\leq \frac{1}{300,000,000,000}$$

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 2, 2007

lec 12W.37

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

The Birthday "Paradox"

In fact, in a term with 6.042 enrollment of 140, we found 17 pairs with same birthday (and 2 triples)

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 2, 2007

lec 12W.38

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

The Birthday "Paradox"

Wait! Whether one pair of students has the same birthday is **not** independent of other pairs: if (Joy, Tim) have same b'day, and (Tim, Mike) do too, then $\Pr\{(\text{Joy, Mike}) \text{ same b'day}\} = 1$.

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 2, 2007

lec 12W.41

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

The Birthday "Paradox"

But this dependence actually makes same b'day pairs *more* likely, so our value for $\Pr\{\text{no matches}\}$ is a valid *upper* bound.

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 2, 2007

lec 12W.42

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

The Birthday "Paradox"

...and when #students \ll # b'days (for example, 23 \ll 365), our bound is tight, because pairs w/same b'day not likely to overlap.

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 2, 2007

lec 12W.43

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Team Problems

Problems

3 & 4

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 2, 2007

lec 12W.42



Introduction to Random Variables

May 4, 2007

Albert R. Meyer, copyright 2007

lec 12F.1



Guess the Bigger Number

Team 1:

- Write different integers between 0 and 7 on two pieces of paper
- Show to Team 2 face down

Team 2:

- Expose one paper and look at number
- Either *stick* or *switch* to other number

Team 2 wins if ends with larger number

May 4, 2007

Albert R. Meyer, copyright 2007

lec 12F.2



Guess the Bigger Number

Try it out!

May 4, 2007

Albert R. Meyer, copyright 2007

lec 12F.3



Strategy for Team 2

Choose papers with equal probability.
If exposed number is "small" then switch; otherwise stick.

"small" means \leq threshold Z .

Z is random integer, $0 \leq Z < 7$.

May 4, 2007

Albert R. Meyer, copyright 2007

lec 12F.4



Analysis of Team 2 Strategy

Case ($\text{low} \leq Z < \text{high}$):

Team 2 wins in this case, so

$\Pr\{\text{Team 2 wins}\} = 1$

and $\Pr\{\text{this case}\} \geq \frac{1}{7}$

May 4, 2007

Albert R. Meyer, copyright 2007

lec 12F.5



Analysis of Team 2 Strategy

Case ($\text{high} \leq Z$):

Team 2 will switch, so

wins iff low card gets exposed.

$\Pr\{\text{Team 2 wins}\} = \frac{1}{2}$

May 4, 2007

Albert R. Meyer, copyright 2007

lec 12F.6

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

Analysis of Team 2 Strategy

Case ($Z < \text{low}$):

Team 2 will stick, so
wins iff high card gets exposed.

$$\Pr\{\text{Team 2 wins}\} = \frac{1}{2}$$

May 4, 2007

Albert R. Meyer, copyright 2007

lec 12F.7

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

Analysis of Team 2 Strategy

So $1/7$ of time, sure win.

Rest of time, 50/50 win, so

$\Pr\{\text{Team 2 wins}\} \geq$

$$\frac{1}{7} \cdot 1 + \frac{6}{7} \cdot \frac{1}{2} = \frac{4}{7} > \frac{1}{2}$$

May 4, 2007

Albert R. Meyer, copyright 2007

lec 12F.8

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

Analysis of Team 2 Strategy

Does not matter
what Team 1 does!!

May 4, 2007

Albert R. Meyer, copyright 2007

lec 12F.9

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

Team Problem

Problem 1

How can Team 1 guarantee

$$\Pr\{\text{Team 2 wins}\} \leq \frac{4}{7}$$

whatever Team 2 does?

May 4, 2007

Albert R. Meyer, copyright 2007

lec 12F.11

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

Random Variables

Informally: an RV is a number
produced by a random process:

- number of larger card
- number of smaller card
- number of exposed card
- threshold variable Z

May 4, 2007

Albert R. Meyer, copyright 2007

lec 12F.12

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

What is a Random Variable?

Formally,

$$\mathbf{R} : \mathcal{S} \rightarrow \mathbb{R}$$

Sample space (usually)

May 4, 2007

Albert R. Meyer, copyright 2007

lec 12F.13

6	9	13	7
10	12	16	5
3	7	8	14
15	4	11	2

Intro to Random Variables

Example: Flip three fair coins.

$C ::=$ number of heads (**C**ount).

$M ::= \begin{cases} 1 & \text{if all } \text{M}atch, \\ 0 & \text{otherwise.} \end{cases}$

May 4, 2007

Albert R. Meyer, copyright 2007

lec 12F.14

6	9	13	7
10	12	16	5
3	7	8	14
15	4	11	2

Intro to Random Variables

Specify events using values of variables.

- $[C = 1]$ is the event "exactly 1 head"
 $\Pr\{C = 1\} = 3/8$
- $\Pr\{C \geq 1\} = 7/8$
- $\Pr\{C \cdot M > 0\} = \Pr\{M > 0 \text{ and } C > 0\}$
 $= \Pr\{\text{all heads}\} = 1/8$

May 4, 2007

Albert R. Meyer, copyright 2007

lec 12F.15

6	9	13	7
10	12	16	5
3	7	8	14
15	4	11	2

Independent Variables

Random variables R, S

are **independent** iff

$[R = a], [S = b]$

are independent *events*

for all numbers a, b .

May 4, 2007

Albert R. Meyer, copyright 2007

lec 12F.16

6	9	13	7
10	12	16	5
3	7	8	14
15	4	11	2

Independent Variables

Alternative version 1: R, S **independent** iff

$\Pr\{R = a \mid S = b\} = \Pr\{R = a\}.$

Alternative version 2:

$\Pr\{R = a \text{ and } S = b\} =$

$\Pr\{R = a\} \cdot \Pr\{S = b\}.$

May 4, 2007

Albert R. Meyer, copyright 2007

lec 12F.17

6	9	13	7
10	12	16	5
3	7	8	14
15	4	11	2

Independent Variables

Tell me:

Are C and M

independent?

May 4, 2007

Albert R. Meyer, copyright 2007

lec 12F.18

6	9	13	7
10	12	16	5
3	7	8	14
15	4	11	2

Independent Variables

$H_1 ::=$ indicator for Head on coin 1

$H_2 ::=$ indicator for Head on coin 2

$P ::= H_1 \oplus H_2 \quad (\text{mod } 2 \text{ sum}).$

any 2 of them are independent:

$\Pr\{P=0 \mid H_2=a\} = 1/2 = \Pr\{P=0\}, \text{ etc.}$

But any 2 **determine the 3rd** one,
so the 3 *together* are not really
independent.

May 4, 2007

Albert R. Meyer, copyright 2007

lec 12F.19

6	9	13	7
10	16	5	
3	1	4	14
15	8	12	2

Independent Variables

Pairwise Independence:

$$\Pr\{A_i=a_i \text{ and } A_j=a_j\} = \Pr\{A_i=a_i\} \cdot \Pr\{A_j=a_j\} \quad \text{all } i \neq j.$$

Mutual Independence:

$$\Pr\{A_1=a_1 \text{ and } A_2=a_2 \text{ and } \cdots A_n=a_n\} = \Pr\{A_1=a_1\} \cdot \Pr\{A_2=a_2\} \cdots \Pr\{A_n=a_n\}.$$

May 4, 2007

Albert R. Meyer, copyright 2007

lec 12F.20

6	9	13	7
10	16	5	
3	1	4	14
15	8	12	2

Independent Variables

k-wise Independence:
any k of the variables are
mutually independent
(so 2-wise = pairwise)

May 4, 2007

Albert R. Meyer, copyright 2007

lec 12F.21

6	9	13	7
10	16	5	
3	1	4	14
15	8	12	2

Independent Variables

Pairwise Independence sufficient
for major applications (in later
lecture).

Good to know, since pairwise holds
in important cases where mutual
does not.

May 4, 2007

Albert R. Meyer, copyright 2007

lec 12F.22

6	9	13	7
10	16	5	
3	1	4	14
15	8	12	2

Team Problems

Problems
2&3

May 4, 2007

Albert R. Meyer, copyright 2007

lec 12F.30

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

Binomial Distribution & Sampling

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

What is a Random Variable?

Formally,

$$R : \mathcal{S} \rightarrow \mathbb{R}$$

Sample space

(usually)

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

Independent Variables

Random variables R, S

are **independent** iff

$$[R = a], [S = b]$$

are independent *events*

for all numbers a, b .

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

Independent Variables

Alternative version:

$$\Pr\{R = a \text{ and } S = b\} = \Pr\{R = a\} \cdot \Pr\{S = b\}.$$

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

Mutually Independent RV's

Mutual Independence of
random vars A_1, A_2, \dots, A_n :

$$\Pr\{A_1=a_1 \text{ and } A_2=a_2 \text{ and } \dots A_n=a_n\} = \Pr\{A_1=a_1\} \cdot \Pr\{A_2=a_2\} \cdots \Pr\{A_n=a_n\}.$$

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

Independent Variables

k-wise Independence:
any k of the variables are
mutually independent
(2-wise = **pairwise**)

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

Independent Variables

Pairwise Independence
sufficient for major
applications (in later lecture)
which is useful since pairwise
holds in important cases where
mutual does not.

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 7, 2007

lec-13M.7

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

Density & Distribution

The **Probability Density Function**
of random variable R ,

$$\text{PDF}_R(a) ::= \Pr\{R=a\}$$

Cumulative Distribution Function of R ,

$$\text{CDF}_R(a) ::= \Pr\{R \leq a\}$$

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 7, 2007

lec-13M.8

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

Indicator Variables

Indicator variable for event A :

$$I_A ::= \begin{cases} 1 & \text{if } A \text{ occurs,} \\ 0 & \text{if } \overline{A} \text{ occurs.} \end{cases}$$

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 7, 2007

lec-13M.11

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

Distributions

Example:

$H_i ::=$ indicator for a head on
the i th coin flip.

Coin may be *biased*:

$$\Pr\{H_i = 1\} = p \neq 1/2$$

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 7, 2007

lec-13M.12

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

Binomial Distribution

$H_{n,p} ::=$ # heads in n mutually
independent flips of a p -biased
coin.

$$H_{n,p} = H_1 + H_2 + \dots + H_n$$

Probability space: the 2^n
sequences of n H's and T's.

$$\Pr\{Q\} ::= p^{\#H's \text{ in } Q} \cdot (1-p)^{\#T's}$$

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 7, 2007

lec-13M.14

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

Binomial Distribution

$$\begin{aligned} \Pr\{k \text{ Heads}\} = & \\ & (\#k \text{ head seqs}) \\ & \cdot \Pr\{\text{seq with } k \text{ H's}\} \end{aligned}$$

$$\text{PDF}_{H_{n,p}}(k) = \binom{n}{k} p^k (1-p)^{n-k}$$

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 7, 2007

lec-13M.16

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

Polling & Sampling

Estimate % contaminated fish in Charles River?



Procedure: catch n fish, test each, use %contaminated in catch as estimate of %contaminated in whole river

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 7, 2007

lec-13M.18

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

Sampling Questions



Catch 100 fish; what is probability that estimate is within 10% of actual%?

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 7, 2007

lec-13M.19

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

Model as Coin Tosses



p ::= fraction contaminated in river
Fish tested: coin toss with bias p .

Catching n fish: tossing n coins

A ::= fraction contaminated in the sample of 100

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 7, 2007

lec-13M.20

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

Polling using Binomial PDF

A = # "heads" / 100
within 10% of p ?

$$\Pr\{|A - p| \leq 0.1\} = \Pr\{|H_{100,p} - 100p| \leq 10\}$$

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 7, 2007

lec-13M.21

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

Polling using Binomial PDF

How do we bound this probability when we don't know p ?

Lemma: $\Pr\{|H_{n,p} - 100p| \leq 10\}$ is min for $p = 1/2$

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 7, 2007

lec-13M.22

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

Compute the exact probability

$$\Pr\{|A - p| \leq 0.1\} \geq$$

$$\Pr\{|H_{100,1/2} - 50| \leq 10\}$$

$$= \sum_{h=40}^{60} \binom{100}{h} 2^{-100} \geq 0.96$$

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 7, 2007

lec-13M.23

6	9	10	7
12	16	5	
3	5	4	14
15	8	11	2

Confidence

We can be **96% confident** that our estimated fraction is within **0.1** of the actual fraction of contaminated fish in the whole river.

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 7, 2007

lec-13M.24

6	9	10	7
12	16	5	
3	5	4	14
15	8	11	2

Sample size for better estimate

Suppose we want an estimate of the fraction that will be **4% (± 0.04)** accurate for **95%** of the time? Similar calculation implies need to sample **589** fish.

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 7, 2007

lec-13M.25

6	9	10	7
12	16	5	
3	5	4	14
15	8	11	2

Confidence – **not** Probable Reality

Now suppose we sample **589** fish and discover **47** are contaminated. So we estimate p is **47/589**.

It's tempting to say

~~"the probability that~~

~~$p = 47/589 \pm 0.04$~~

~~is at least 95%"~~

--Technically not correct!

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 7, 2007

lec-13M.26

6	9	10	7
12	16	5	
3	5	4	14
15	8	11	2

Confidence

p is the actual fraction of bad fish in the river.

p is **unknown**,

but not a random variable!

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 7, 2007

lec-13M.27

6	9	10	7
12	16	5	
3	5	4	14
15	8	11	2

Confidence

The possible outcomes of our *sampling procedure* is a random variable. We can say that "the **probability** that **our sample fraction** will be within ± 0.04 of the true fraction is at least **95%**"

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 7, 2007

lec-13M.28

6	9	10	7
12	16	5	
3	5	4	14
15	8	11	2

Confidence

For simplicity we say that

$p = 47/589 \pm 0.04$ at the **95% confidence level**

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 7, 2007

lec-13M.29

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

Binomial Approximation

Numerical approximations
for $\text{PDF}_{H_{n,p}}(\alpha n)$,
 $\text{CDF}_{H_{n,p}}(\alpha n)$,
in Notes 13.

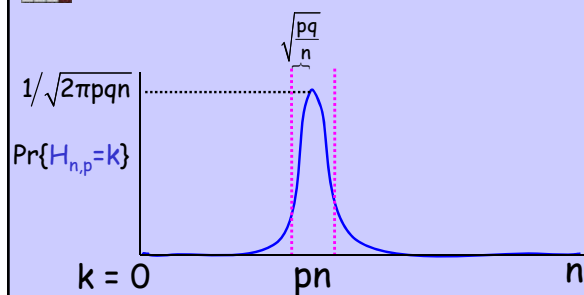
Copyright © 2007, Albert R. Meyer. All rights reserved.

May 7, 2007

lec-13M-20

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

Distribution of Heads



Copyright © 2007, Albert R. Meyer. All rights reserved.

May 7, 2007

lec-13M-21

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

Binomial Approximation

Messy formulas, but **easy to compute**.

Exact answers for n more than a few 1000 are impossible to compute
(requires arithmetic on million-digit numbers)

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 7, 2007

lec-13M-24

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

Team Problems

Problems 1&2

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 7, 2007

lec-13M-35

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

Team Problems

Problems 1&2

Copyright © Albert R. Meyer, 2007. All rights reserved.

May 9, 2007

lec 13w.1

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

Mathematics for Computer Science
MIT 6.042J/18.062J

Great Expectations

Copyright © Albert R. Meyer, 2007. All rights reserved.

May 9, 2007

lec 13w.2

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

Carnival Dice



Choose a number from 1 to 6,
then roll 3 fair dice:

win \$1 if any die matches num

lose \$1 if no match. *Example:*

choose number 2, roll 2,4,2,
win \$1

Copyright © Albert R. Meyer, 2007. All rights reserved.

May 9, 2007

lec 13w.4

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

Carnival Dice



Is this a fair game?

Copyright © Albert R. Meyer, 2007. All rights reserved.

May 9, 2007

lec 13w.5

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

Carnival Dice



Clearly NOT fair:
 $\text{pr}\{\text{win}\} = 1 - (5/6)^3 < 0.43 < 1/2$

Copyright © Albert R. Meyer, 2007. All rights reserved.

May 9, 2007

lec 13w.6

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

Carnival Dice, II



Choose a number from 1 to 6,
then roll 3 fair dice:

win \$1 for each match

lose \$1 if no match. *Example:*

choose number 2, roll 2,4,2,
win \$2

Copyright © Albert R. Meyer, 2007. All rights reserved.

May 9, 2007

lec 13w.7

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

Carnival Dice, II



Is this now a **fair game**?

Copyright © Albert R. Meyer, 2007. All rights reserved.

May 9, 2007

lec 13w.8

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

Carnival Dice, II

$\Pr\{0 \text{ matches}\} =$	$\left(\frac{5}{6}\right)^3$	<u>win</u>
$\Pr\{1 \text{ match}\} =$	$\binom{3}{1} \left(\frac{1}{6}\right) \left(\frac{5}{6}\right)^2$	-1
$\Pr\{2 \text{ matches}\} =$	$\binom{3}{2} \left(\frac{1}{6}\right)^2 \left(\frac{5}{6}\right)$	1
$\Pr\{3 \text{ matches}\} =$	$\binom{3}{3} \left(\frac{1}{6}\right)^3$	2
		3

Copyright © Albert R. Meyer, 2007. All rights reserved.

May 9, 2007

lec 13w.10

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

Carnival Dice, II

Average win:

$$\frac{(5^3 \cdot -1) + 3 \cdot 5^2 \cdot 1 + 3 \cdot 5 \cdot 2 + 3}{6^3} = -\frac{17}{216} \approx -8 \text{ cents}$$

NOT fair!

Copyright © Albert R. Meyer, 2007. All rights reserved.

May 9, 2007

lec 13w.11

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

Carnival Dice, II

You can "**expect**" to lose 8 cents per play.

Notice that you **never** actually lose 8 cents on any single play.

Rather, this is what you expect to lose **on average**.

Copyright © Albert R. Meyer, 2007. All rights reserved.

May 9, 2007

lec 13w.12

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

Expectation

The **expected value** of a random variable **D** is: the **average value** of **D** --with values weighted by their probabilities.

Copyright © Albert R. Meyer, 2007. All rights reserved.

May 9, 2007

lec 13w.13

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

Expectation

expected value also called **mean value**, **mean**, or **expectation**

Copyright © Albert R. Meyer, 2007. All rights reserved.

May 9, 2007

lec 13w.14

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

Expectation

The **expected value** of a random variable D is:

$$E[D] ::= \sum_v v \cdot \Pr\{D = v\}$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

May 9, 2007

lec 13w.15

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

Sum or Integral?

In the most general probability spaces, the sum would have to be an integral. We can get away with sums because we assume the sample space is **countable**:

$$\mathcal{S} = \{\omega_0, \omega_1, \dots, \omega_n, \dots\}$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

May 9, 2007

lec 13w.16

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

Sum or Integral?

$$\Pr\{D = v\} ::= \sum_{D(\omega)=v} \Pr\{\omega\}$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

May 9, 2007

lec 13w.17

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

Expectation

So

$$\begin{aligned} E[D] &::= \sum_v v \cdot \Pr\{D = v\} \\ &= \sum_{\omega \in \mathcal{S}} D(\omega) \cdot \Pr\{\omega\} \end{aligned}$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

May 9, 2007

lec 13w.18

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

Mean Time to Failure

Biased coin with $\Pr\{\text{Head}\} = p$.
Flip until a Head comes up.
Expected #flips?

Copyright © Albert R. Meyer, 2007. All rights reserved.

May 9, 2007

lec 13w.19

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

Mean Time to Failure

$\Pr\{\text{1st Head on flip 1}\} = p,$
 $\Pr\{\text{1st Head on flip 2}\} = (1-p)p,$
 $\Pr\{\text{1st Head on flip 3}\} = (1-p)^2p,$
 \vdots
 $\Pr\{\text{1st Head on flip } n\} = (1-p)^{n-1}p.$

Copyright © Albert R. Meyer, 2007. All rights reserved.

May 9, 2007

lec 13w.20

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

Mean Time to Failure

E [# flips till 1st Head]

$$= \sum_{n=1}^{\infty} n \cdot (1-p)^{n-1} p$$

$$= p \left(\sum_{n=0}^{\infty} (n+1) \cdot (1-p)^n \right)$$

Copyright © Albert R. Meyer, 2007. All rights reserved.

May 9, 2007

lec 13w.21

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

Mean Time to Failure

E [# flips till 1st Head]

$$= p \left(\frac{1}{(1 - (1-p))^2} \right)$$

$$= \frac{1}{p}$$

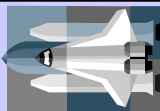
Copyright © Albert R. Meyer, 2007. All rights reserved.

May 9, 2007

lec 13w.22

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

Mean Time to Failure



application: Space station Mir
say had 1/150,000 chance of
exploding in any given hour.
After how many hours did
we expect it to explode?
150,000 hours \approx 17 years

Copyright © Albert R. Meyer, 2007. All rights reserved.

May 9, 2007

lec 13w.23

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

Team Problems

Problems 3–5

Copyright © Albert R. Meyer, 2007. All rights reserved.

May 9, 2007

lec 13w.24

Calculating Expectations

May 11, 2007

copyright Albert R Meyer
2007

Combining Expectations

May

- I is an indicator vble.

$$\begin{aligned} E[I] &::= 0 \cdot \Pr\{I=0\} + 1 \cdot \Pr\{I=1\} \\ &= \Pr\{I=1\} \end{aligned}$$

- Linearity 1) $E[R+S] = E[R] + E[S]$
 R, S need NOT be independent.

$$2) E[3R] = 3E[R]$$

$$\begin{aligned} \text{Pf: } E[3R] &= \sum_{\omega \in \Omega} 3R(\omega) \cdot \Pr\{\omega\} \\ &= 3 \cdot \underbrace{\sum_{\omega} R(\omega) \cdot \Pr(\omega)}_{=:: E[R]} \end{aligned}$$

$$E[H_{n,p}] = E[H_1 + H_2 + \dots + H_n] \\ = n E[H_1] = np$$

$$E[\# \text{ b'days in class of } n \text{ students}] =$$

$S_{ij} ::=$ ^{pairs} i^{th} & j^{th} student have same b'day.

$$E[S_{ij}] = \frac{1}{365}$$

$$E[\sum S_{ij}]$$

$$= (\# S_{ij}) \cdot \frac{1}{365}$$

$$= \binom{n}{2} / 365$$

$$n=27 \quad E[\# \text{ matching b'days}] \approx 1$$

$$n=80 \quad E[\text{ " }] \approx 8.9$$

Conditional Expectation:

$$E[R|A] ::= \sum_r r \cdot \Pr\{R=r|A\}$$

Law Total Expect:

~~$$E[R] = E[R|A] \cdot \Pr\{A\} + E[R|\bar{A}] \cdot \Pr\{\bar{A}\}$$~~

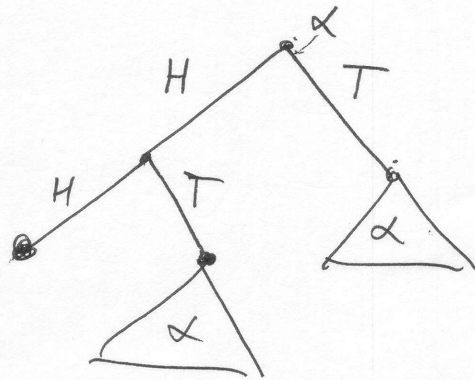
$$E[R] = E[R|A] \cdot \Pr\{A\} + E[R|\bar{A}] \cdot \Pr\{\bar{A}\}$$

Pf:

$$\begin{aligned} & \Pr\{A\} \cdot \sum_r r \cdot \Pr\{R=r|A\} + \Pr\{\bar{A}\} \cdot \sum_r r \cdot \Pr\{R=r|\bar{A}\} \\ &= \sum_r r \cdot \Pr\{R=r|A\} \cdot \Pr\{A\} + \dots \\ &= \sum_r r \cdot \Pr\{R=r \text{ and } A\} + \sum_r r \cdot \Pr\{R=r \text{ and } \bar{A}\} \\ &= \sum_r r \cdot [\Pr\{R=r \text{ and } A\} + \Pr\{R=r \text{ and } \bar{A}\}] \\ &= \sum_r r \cdot [\Pr\{R=r\}] ::= E[R] \end{aligned}$$

HH v HT

stop at HH:



$$E[x] = 2 \cdot \frac{1}{4} + (E[x] + 2) \cdot \frac{1}{4} + (1 + E[x]) \cdot \frac{1}{2}$$

$$E = \frac{1}{2} + \frac{E}{4} + \frac{1}{2} + \frac{1}{2} + \frac{E}{2}$$

$$\frac{E}{4} = \frac{3}{2} = 6$$



Deviation from the Mean



Don't expect the Expectation!

Toss **101** fair coins.
 $E[\#H] = 50.5$



Don't expect the Expectation!

$\Pr\{\text{exactly } 50.5 \text{ Heads}\} = 0$
 $\Pr\{\text{exactly } 50 \text{ Heads}\} < 1/13$
 $\Pr\{50.5 \pm 1 \text{ Heads}\} < 1/7$



Don't expect the Expectation!

Toss **1001** fair coins.
 $E[\#H] = 500.5$
 $\Pr\{\#H = 500\} < 1/39$
 $\Pr\{\#H = 500.5 \pm 1\} < 1/19$
 smaller



Within a % of the mean?

Toss **1001** fair coins of 1001
 $\Pr\{\#H = 500 \pm 1\%\}$
 $= \Pr\{\#H = 500 \pm 10\}$
 ≈ 0.49
not so bad



Giving *Meaning* to the "Mean"

Let $\mu ::= E[R]$
 • What is $\Pr\{R \text{ far from } \mu\}$?
 $\Pr\{|R - \mu| > x\}$
 • R's average deviation?
 $E[|R - \mu|]$?

6	9	13	7
12		10	5
3	1	14	11
15	8	16	4

Two Dice with Same Mean

Fair Die

$$\bullet E[D_1] = 3.5$$

Loaded Die throwing only 1 & 6:

$$\bullet E[D_2] = (1+6)/2 = 3.5 \text{ also!}$$



Copyright © Albert R. Meyer, 2007. All rights reserved. May 14, 2007

lec 14M.8

6	9	13	7
12		10	5
3	1	14	11
15	8	16	4

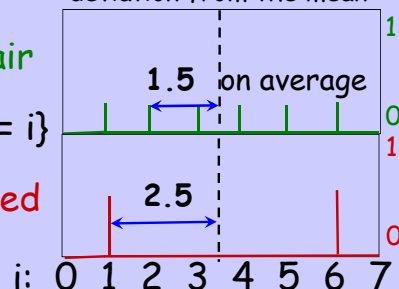
Two Dice with Same Mean

deviation from the mean

Fair

$\Pr\{D = i\}$

Loaded



Copyright © Albert R. Meyer, 2007. All rights reserved. May 14, 2007

lec 14M.9

6	9	13	7
12		10	5
3	1	14	11
15	8	16	4

Dice have Different Deviations

Fair Die:

$$E[|D_1 - \mu|] = 1.5$$

Loaded Die:

$$E[|D_2 - \mu|] = 2.5$$

Copyright © Albert R. Meyer, 2007. All rights reserved. May 14, 2007

lec 14M.10

6	9	13	7
12		10	5
3	1	14	11
15	8	16	4

Giving Meaning to the "Mean"

The mean alone is not a good predictor of D 's behavior. We generally need more about its distribution, especially probable deviation from its mean.

Copyright © Albert R. Meyer, 2007. All rights reserved. May 14, 2007

lec 14M.11

6	9	13	7
12		10	5
3	1	14	11
15	8	16	4

Example: IQ

IQ measure was constructed so that

average IQ = 100.

What fraction of the people can *possibly* have an IQ ≥ 300 ?

Copyright © Albert R. Meyer, 2007. All rights reserved. May 14, 2007

lec 14M.15

6	9	13	7
12		10	5
3	1	14	11
15	8	16	4

IQ Higher than 300?

Fraction f with IQ ≥ 300 adds $\geq 300f$ to average, so $100 = \text{avg IQ} \geq 300f$:

$$f \leq 100/300 = 1/3$$

Copyright © Albert R. Meyer, 2007. All rights reserved. May 14, 2007

lec 14M.16

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

IQ Higher than 300?

At most $\frac{1}{3}$ of people
have $\text{IQ} \geq 300$

$$\Pr\{\text{IQ} \geq 300\} \leq \frac{E[\text{IQ}]}{300}$$

Copyright © Albert R. Meyer, 2007. All rights reserved. May 14, 2007

lec 14M.17

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

IQ Higher than x?

In general,

$$\Pr\{\text{IQ} \geq x\} \leq \frac{100}{x}$$

Copyright © Albert R. Meyer, 2007. All rights reserved. May 14, 2007

lec 14M.18

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

IQ Higher than x?

Besides mean = 100,
we used *only one fact about the
distribution* of IQ:

IQ is always nonnegative

Copyright © Albert R. Meyer, 2007. All rights reserved. May 14, 2007

lec 14M.19

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

Markov Bound

If R is nonnegative, then

$$\Pr\{R \geq x\} \leq \frac{E[R]}{x}$$

for $x > 0$.

Copyright © Albert R. Meyer, 2007. All rights reserved. May 14, 2007

lec 14M.20

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

Markov Bound

- Weak
- Obvious
- Useful anyway

Copyright © Albert R. Meyer, 2007. All rights reserved. May 14, 2007

lec 14M.22

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

$\text{IQ} \geq 300$, again

Suppose we are *given* that IQ
is always ≥ 40 ?

Get a better bound on fraction
 f with $\text{IQ} \geq 300$, by considering
 $\text{IQ} - 40$
since this is now ≥ 0 .

Copyright © Albert R. Meyer, 2007. All rights reserved. May 14, 2007

lec 14M.23

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

IQ ≥ 300 , again

f contributes **300f** to the average of **IQ-40**, so

$$60 = E[\text{IQ}-40] \geq 300f$$

$$f \leq 60/300 = 1/5$$

Better bound from Markov by shifting R to have 0 as minimum

Copyright © Albert R. Meyer, 2007. All rights reserved. May 14, 2007

lec 14M.26

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

Improving the Markov Bound

$$\Pr\{|R-\mu| \geq x\} = \Pr\{(R-\mu)^2 \geq x^2\}$$

by Markov:

$$\leq \frac{E[(R-\mu)^2]}{x^2}$$

variance of R

Copyright © Albert R. Meyer, 2007. All rights reserved. May 14, 2007

lec 14M.27

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

Chebyshev Bound

$$\Pr\{|R-\mu| \geq x\} \leq \frac{\text{Var}[R]}{x^2}$$

Copyright © Albert R. Meyer, 2007. All rights reserved. May 14, 2007

lec 14M.28

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

Variance of an Indicator

I an indicator with $E[I]=p$:

$$\begin{aligned} \text{Var}[I] &::= E[(I-p)^2] \\ &= E[I^2 - 2pI + p^2] \\ &= E[I^2] - 2p + p^2 \\ &= p - 2p + p^2 = p(1-p). \end{aligned}$$

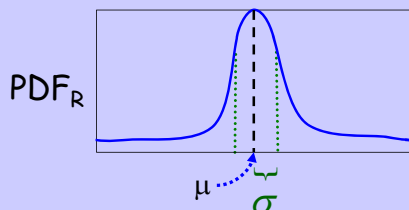
Copyright © Albert R. Meyer, 2007. All rights reserved. May 14, 2007

lec 14M.29

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

Variance and Standard Deviation

$$\sigma_R ::= \sqrt{\text{Var}[R]}$$



Copyright © Albert R. Meyer, 2007. All rights reserved. May 14, 2007

lec 14M.30

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

Standard Deviation

$$\Pr\{|R-\mu| \geq x\} \leq \frac{\sigma^2}{x^2}$$

R probably not many σ 's from μ :
further than σ $\Pr \leq 1$

$$2\sigma \quad \Pr \leq 1/4$$

$$3\sigma \quad \Pr \leq 1/9$$

$$4\sigma \quad \Pr \leq 1/16$$

Copyright © Albert R. Meyer, 2007. All rights reserved. May 14, 2007

lec 14M.32

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Calculating Variance

$$\text{Var}[aR + b] = a^2 \text{Var}[R]$$

$$\text{Var}[R] = E[R^2] - E^2[R]$$

(simple proofs applying linearity of expectation to the def of variance)

Copyright © Albert R. Meyer, 2007. All rights reserved. May 14, 2007

lec 14M.34

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Calculating Variance

$$\text{Var}[R_1 + R_2 + \dots + R_n] = \text{Var}[R_1] + \text{Var}[R_2] + \dots + \text{Var}[R_n]$$

providing R_1, R_2, \dots, R_n are pairwise independent

Copyright © Albert R. Meyer, 2007. All rights reserved. May 14, 2007

lec 14M.35

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Calculating Variance

Pairwise Independent Additivity

similar proof using linearity of expectation & def of variance

Copyright © Albert R. Meyer, 2007. All rights reserved. May 14, 2007

lec 14M.37

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Team Problems

Problems 1–5

Copyright © Albert R. Meyer, 2007. All rights reserved. May 14, 2007

lec 14M.38

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

Team Problems

Problems 1&2

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 16, 2007

lec 14W.1

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

Mathematics for Computer Science

MIT 6.042J/18.062J

Deviation of Repeated Trials

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 16, 2007

lec 14W.2

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

Jacob D. Bernoulli (1659 - 1705)

Even the stupidest man —by some instinct of nature *per se* and by no previous instruction (this is truly amazing) —knows for sure that the more observations ...that are taken, the less the danger will be of straying from the mark.

---*Ars Conjectandi* (The Art of Guessing), 1713*

*taken from Grinstead & Snell,
http://www.dartmouth.edu/~chance/teaching_aids/books_articles/probability_book/book.html
Introduction to Probability, American Mathematical Society, p. 310.

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 16, 2007

lec 14W.3

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

Jacob D. Bernoulli (1659 - 1705)

It certainly remains to be inquired whether after the number of observations has been increased, the probability...of obtaining the true ratio...finally exceeds any given degree of certainty; or whether the problem has, so to speak, its own asymptote---that is, whether some degree of certainty is given which one can never exceed.

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 16, 2007

lec 14W.4

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

Repeated Trials

Random variable R with mean μ
 n independent observations of R

$$R_1, \dots, R_n$$

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 16, 2007

lec 14W.5

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

Repeated Trials

take average:

$$A_n ::= \frac{R_1 + \dots + R_n}{n}$$

close to 'true ratio' with prob. ?

$$\Pr\{|A_n - \mu| \leq x\} ?$$

as close as $x > 0$

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 16, 2007

lec 14W.6

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

Repeated Trials

$$\Pr\{|A_n - \mu| \leq x\}$$

Even 'stupidest man' knows this prob.
gets bigger as n gets bigger
—but *how big?*

Does it "exceed... any given degree of
certainty"?

That is, does it **approach 1**?

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 16, 2007

lec 14W.7

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

Weak Law of Large Numbers

$$\lim_{n \rightarrow \infty} \Pr\{|A_n - \mu| \leq x\} = 1$$

YES

$$\lim_{n \rightarrow \infty} \Pr\{|A_n - \mu| > x\} = 0$$

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 16, 2007

lec 14W.8

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

Jacob D. Bernoulli (1659 - 1705)

Therefore, this is the problem which I
now set forth and make known after I
have pondered over it for twenty years.
Both its novelty and its very great
usefulness, coupled with its just as
great difficulty, can exceed in
weight and value all the remaining
chapters of this thesis.

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 16, 2007

lec 14W.9

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

Jacob D. Bernoulli (1659 - 1705)



Copyright © 2007, Albert R. Meyer. All rights reserved.

May 16, 2007

lec 14W.10

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

Weak Law of Large Numbers

$$\lim_{n \rightarrow \infty} \Pr\{|A_n - \mu| > x\} = 0$$

Will be an easy Corollary of Chebyshev
and properties of variance.

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 16, 2007

lec 14W.11

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

Repeated Trials

$$\begin{aligned} E[A_n] &= E\left[\frac{R_1 + \cdots + R_n}{n}\right] \\ &= \frac{E[R_1] + \cdots + E[R_n]}{n} \\ &= \frac{n\mu}{n} = \mu \end{aligned}$$

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 16, 2007

lec 14W.12

6	9	13	7
12	10	5	
3	4	8	14
15	11	16	2

Repeated Trials

by Chebyshev:

$$\Pr\{|A_n - \mu| > x\} \leq \frac{\text{Var}[A_n]}{x^2}$$

so need only show
 $\text{Var}[A_n] \rightarrow 0$

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 16, 2007

lec 14W.13

6	9	13	7
12	10	5	
3	4	8	14
15	11	16	2

Repeated Trials

what is $\text{Var}[A_n]$?

let $\sigma^2 ::= \text{Var}[R]$

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 16, 2007

lec 14W.14

6	9	13	7
12	10	5	
3	4	8	14
15	11	16	2

Repeated Trials

$\text{Var}[A_n]$

$$= \text{Var}[(R_1 + \dots + R_n) / n]$$

$$= (\text{Var}[R_1] + \dots + \text{Var}[R_n]) / n^2$$

$$= \frac{n\sigma^2}{n^2} = \frac{\sigma^2}{n}$$

$\rightarrow 0$ as $n \rightarrow \infty$

QED

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 16, 2007

lec 14W.15

6	9	13	7
12	10	5	
3	4	8	14
15	11	16	2

Analysis of the Proof

proof only used

- R_1, \dots, R_n have same finite mean, μ
- and finite variance, σ^2
- and variances add:

$$\text{Var}[R_1 + \dots + R_n]$$

$$= \text{Var}[R_1] + \dots + \text{Var}[R_n]$$

which follows from *pairwise* independence

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 16, 2007

6	9	13	7
12	10	5	
3	4	8	14
15	11	16	2

Pairwise Independent Sampling

Let R_1, \dots, R_n be pairwise independent random vars with the same finite mean, μ , and variance, σ^2 . Let

$A_n ::= (R_1 + \dots + R_n) / n$. Then

$$\Pr\{|A_n - \mu| > x\} \leq \frac{1}{n} \left(\frac{\sigma}{x}\right)^2$$

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 16, 2007

6	9	13	7
12	10	5	
3	4	8	14
15	11	16	2

Pairwise Independent Sampling

The punchline:

we now know how big a sample is needed to estimate the mean of any* random variable to within any* desired tolerance and to any* degree of confidence.

* $\text{Var}[\text{rand. var}] < \infty$, tolerance > 0 , confidence $< 100\%$

Copyright © 2007, Albert R. Meyer. All rights reserved.

May 16, 2007

6	12	7
18	16	5
9	4	14
15	11	3

Team Problems

Problems 3&4

Copyright ©2007, Albert R. Meyer. All rights reserved.

May 16, 2007

lec 14W.19