Solutions to In-Class Problems Week 1, Wed.

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

(a) $1/8 > 1/4$.

Bogus proof.

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

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

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

(b) $1¢ = \$0.01 = (\$0.1)^2 = (10¢)^2 = 100¢ = \$1$.

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

Problem 2.

Proposition (Arithmetic-Geometric Mean Inequality)**.** *For all nonnegative real numbers a and b*

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

What is wrong with the following proof of this proposition?

[1] From Stueben, Michael and Diane Sandford. *Twenty Years Before the Blackboard*, Math. Assoc America, ©1998.

Bogus proof.

$$\begin{aligned}
\frac{a+b}{2} &\stackrel{?}{\geq} \sqrt{ab} \\
a+b &\stackrel{?}{\geq} 2\sqrt{ab} \\
a^2+2ab+b^2 &\stackrel{?}{\geq} 4ab \\
a^2-2ab+b^2 &\stackrel{?}{\geq} 0 \\
(a-b)^2 &\geq 0
\end{aligned}$$

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

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

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

Proof.

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

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

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

False Claim.

$$0 = 1.$$

Bogus proof.

$$\begin{aligned} 0 &\stackrel{?}{=} 1 \\ 1 &\stackrel{?}{=} 0 \\ 0+1 &\stackrel{?}{=} 1+0 \\ 1 &= 1 \end{aligned}$$

and the last equality is trivially true. □

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

Bogus proof.

$$\begin{aligned} \frac{a+b}{2} &\stackrel{?}{\geq} \sqrt{ab} \\ 0 \cdot \frac{a+b}{2} &\stackrel{?}{\geq} 0 \cdot \sqrt{ab} \\ 0 &\geq 0 \end{aligned}$$

□

So watch out for backward proofs! ■

Solutions to In-Class Problems Week 2, Wed.

Problem 1. For each of the logical formulas, indicate whether or not it is true when the domain of discourse is $\mathbb{N}$ (the natural numbers 0, 1, 2, ...), $\mathbb{Z}$ (the integers), $\mathbb{Q}$ (the rationals), $\mathbb{R}$ (the real numbers), and $\mathbb{C}$ (the complex numbers).

$$\begin{array}{rlrcl} & \exists x & (x^2 & = & 2) \\ \forall x & \exists y & (x^2 & = & y) \\ \forall y & \exists x & (x^2 & = & y) \\ \forall x \neq 0 & \exists y & (xy & = & 1) \\ \exists x & \exists y & (x+2y & = & 2) \wedge (2x+4y=5) \end{array}$$

Solution.

Statement	$\mathbb{N}$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{C}$
$\exists x\ (x^2 = 2)$	f	f	f	$t\ (x = \sqrt{2})$	t
$\forall x \exists y\ (x^2 = y)$	t	t	t	$t\ (y = x^2)$	t
$\forall y \exists x\ (x^2 = y)$	f	f	f	f (take $y < 0$)	t
$\forall x \neq 0 \exists y\ (xy = 1)$	f	f	t	$t\ (y = 1/x)$	t
$\exists x \exists y\ (x + 2y = 2) \wedge (2x + 4y = 5)$	f	f	f	f	f

■

Problem 2. The goal of this problem is to translate some assertions about binary strings into logic notation. The domain of discourse is the set of all finite-length binary strings: λ, 0, 1, 00, 01, 10, 11, 000, 001, ... (Here λ denotes the empty string.) In your translations, you may use all the ordinary logic symbols (including =), variables, and the binary symbols `0`, `1` denoting 0, 1.

A string like $\texttt{01}x\texttt{0}y$ of binary symbols and variables denotes the *concatenation* of the symbols and the binary strings represented by the variables. For example, if the value of x is `011` and the value of y is `1111`, then the value of $\texttt{01}x\texttt{0}y$ is the binary string `0101101111`.

Here are some examples of formulas and their English translations. Names for these predicates are listed in the third column so that you can reuse them in your solutions (as we do in the definition of the predicate NO-1S below).

Meaning	Formula	Name
x is a prefix of y	$\exists z\ (xz = y)$	PREFIX(x, y)
x is a substring of y	$\exists u \exists v\ (uxv = y)$	SUBSTRING(x, y)
x is empty or a string of 0's	$\neg$SUBSTRING$(1, x)$	NO-1S(x)

(a) x consists of three copies of some string.

Solution. $\exists y\ (x = yyy)$ ■

(b) x is an even-length string of 0's.

Solution. NO-1S$(x) \wedge \exists y\ (x = yy)$ ■

(c) x does not contain both a 0 and a 1.

Solution. $\neg[\text{SUBSTRING}(0, x) \wedge \text{SUBSTRING}(1, x)]$

■

(d) x is the binary representation of $2^k + 1$ for some integer $k \geq 0$.

Solution. $(x = 10) \vee (\exists y\ (x = 1y1 \wedge \text{NO-1S}(y)))$ ■

(e) An elegant, slightly trickier way to define NO-1S(x) is:

$$\text{PREFIX}(x, 0x). \qquad (*)$$

Explain why (*) is true only when x is a string of 0's.

Solution. Prefixing x with 0 rightshifts all the bits. So the nth symbol of x shifts into the $(n+1)$st symbol of $0x$. Now for x to be a prefix of $0x$, the $n+1$st symbol of $0x$ must match the $(n+1)$st symbol of x. So if x satisfies (*), the nth and $(n+1)$st symbols of x must match. This holds for all $n > 0$ up to the length of x, that is, *all* the symbols of x must be the same. In addition, if $x \neq \lambda$, it must start with 0. Therefore, if x satisfies (*), all its symbols must be 0's.

Note that it's easy to see, conversely, that if $x = \lambda$ or x is all 0's, then of course it satisfies (*). ■

Problem 3. A media tycoon has an idea for an all-news television network called LNN: The Logic News Network. Each segment will begin with a definition of the domain of discourse and a few predicates. The day's happenings can then be communicated concisely in logic notation. For example, a broadcast might begin as follows:

> "THIS IS LNN. The domain of discourse is $\{\text{Bill}, \text{Monica}, \text{Ken}, \text{Linda}, \text{Betty}\}$. Let $D(x)$ be a predicate that is true if x is deceitful. Let $L(x, y)$ be a predicate that is true if x likes y. Let $G(x, y)$ be a predicate that is true if x gave gifts to y."

Complete the broadcast by translating the following statements into logic notation.

(a) If neither Monica nor Linda is deceitful, then Bill and Monica like each other.

Solution.

$$(\neg(D(\text{Monica}) \vee D(\text{Linda}))) \longrightarrow (L(\text{Bill}, \text{Monica}) \wedge L(\text{Monica}, \text{Bill}))$$

■

(b) Everyone except for Ken likes Betty, and no one except Linda likes Ken.

Solution.

$$\forall x\ (x = \text{Ken} \wedge \neg L(x, \text{Betty})) \vee (x \neq \text{Ken} \wedge L(x, \text{Betty})) \wedge$$
$$\forall x\ (x = \text{Linda} \wedge L(x, \text{Ken})) \vee (x \neq \text{Linda} \wedge \neg L(x, \text{Ken}))$$

■

(c) If Ken is not deceitful, then Bill gave gifts to Monica, and Monica gave gifts to someone.

Solution.

$$\neg D(\text{Ken}) \longrightarrow (G(\text{Bill}, \text{Monica}) \wedge \exists\, x G(\text{Monica}, x))$$

■

(d) Everyone likes someone and dislikes someone else.

Solution.

$$\forall x \exists y \exists z\ (y \neq z) \wedge L(x, y) \wedge \neg L(x, z)$$

■

(e) How could you express "Everyone except for Ken likes Betty" using just propositional connectives *without* using any quantifiers ($\forall, \exists$)? Can you generalize to explain how *any* logical formula over this domain of discourse can be expressed without quantifiers? How big would the formula in the previous part be if it was expressed this way?

Solution.

$$L(\text{Bill}, \text{Betty}) \wedge L(\text{Monica}, \text{Betty}) \wedge L(\text{Linda}, \text{Betty}) \wedge L(\text{Betty}, \text{Betty}) \wedge \neg L(\text{Ken}, \text{Betty})$$

In general, quantifiers can be eliminated by treating $\forall x\ P(x)$ as an abbreviation for

$$P(\text{Bill}) \wedge P(\text{Monica}) \wedge P(\text{Ken}) \wedge P(\text{Linda}) \wedge P(\text{Betty}),$$

and $\exists x\ P(x)$ as an abbreviation for

$$P(\text{Bill}) \vee P(\text{Monica}) \vee P(\text{Ken}) \vee P(\text{Linda}) \vee P(\text{Betty}).$$

Expanded this way, the three-quantifier formula of the previous part would expand by a factor of $5 \times 5 \times 5 = 125$. So using quantifiers can pay off even when they are not strictly necessary. ■

Problem 4. **(a)** Explain why

$$(\forall z.\ P(z,z)) \longrightarrow \forall x \exists y.\ P(x,y) \tag{1}$$

is valid.

Solution. *Proof.* Assume

$$\forall z.\ P(z,z) \tag{2}$$

is true for some domain and interpretation of the predicate P. We want to show that

$$\forall x \exists y.\ P(x,y) \tag{3}$$

also holds.

So let c be an element of the domain. Then $P(c,c)$ holds by assumption (2). So there is a y, namely $y = c$ such that $P(c,y)$ holds. That is, $\exists y.\ P(c,y)$ is true. But c could have been any element in the domain, so (by *Universal Generalization*), we conclude that (3) holds. □

■

(b) Describe a counter-model demonstrating that

$$(\forall x \exists y.\ P(x,y)) \longrightarrow \forall z.\ P(z,z)$$

is not valid.

Solution. Let $P(x,y)$ mean $x \neq y$. Then the conclusion $\forall z.\ z \neq z$ is always false, but in any domain with two or more elements, the hypothesis is true. ■

Solutions to In-Class Problems Week 3, Wed.

Problem 1. Use induction to prove that

$$1^3 + 2^3 + \ldots + n^3 = \left(\frac{n(n+1)}{2}\right)^2. \tag{1}$$

for all $n \geq 1$.

Remember to formally

1. Declare proof by induction.
2. Identify the induction hypothesis $P(n)$.
3. Establish the base case.
4. Prove that $P(n) \Rightarrow P(n+1)$.
5. Conclude that $P(n)$ holds for all $n \geq 1$.

as in the five part template.

Solution. We proceed by induction. The induction hypothesis, $P(n)$, will be the equation (1).

Base case: First, we must show that $P(1)$ is true. This is immediate, since:

$$1^3 = \left(\frac{1(1+1)}{2}\right)^2$$

Inductive step: Next, we must show that $P(n)$ implies $P(n+1)$ for all $n \geq 1$. Assuming that $P(n)$ is true, we can reason as follows:

$$\begin{aligned} 1^3 + 2^3 + \ldots + n^3 + (n+1)^3 &= \left(\frac{n(n+1)}{2}\right)^2 + (n+1)^3 \\ &= \left(\frac{(n+1)(n+2)}{2}\right)^2 \end{aligned}$$

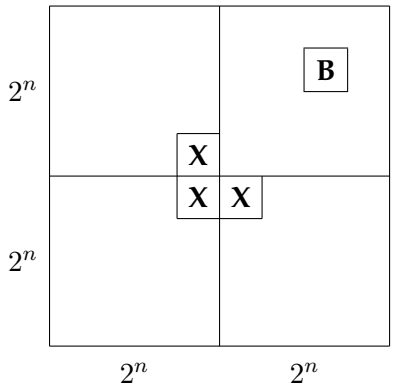
The first step uses the assumption $P(n)$, and the second uses only algebra. This shows that $P(n+1)$ is true. Therefore, $P(n)$ is true for all $n \geq 1$ by induction. ■

Problem 2. **(a)** Prove by induction that a $2^n \times 2^n$ courtyard with a 1×1 statue of Bill in *any position* can be covered with L-shaped tiles.

Solution. Let $P(n)$ be the proposition that for every location of Bill in a $2^n \times 2^n$ courtyard, there exists a tiling of the remainder.

Base case: $P(0)$ is true because Bill fills the whole courtyard.

Inductive step: Asume that $P(n)$ is true for some $n \geq 0$; that is, for every location of Bill in a $2^n \times 2^n$ courtyard, there exists a tiling of the remainder. Divide the $2^{n+1} \times 2^{n+1}$ courtyard into four quadrants, each $2^n \times 2^n$. One quadrant contains Bill (**B** in the diagram below). Place a temporary Bill (**X** in the diagram) in each of the three central squares lying outside this quadrant:



Now we can tile each of the four quadrants by the induction assumption. Replacing the three temporary Bills with a single L-shaped tile completes the job. This proves that $P(n)$ implies $P(n+1)$ for all $n \geq 0$. The theorem follows as a special case.

This proof has two nice properties. First, not only does the argument guarantee that a tiling exists, but also it gives a recursive procedure for finding such a tiling. Second, we have a stronger result: if Bill wanted a statue on the edge of the courtyard, away from the pigeons, we could accommodate him! ■

(b) *(Discussion Question)* In part (a) we saw that it can be easier to prove a stronger theorem. Does this surprise you? How would you explain this phenomenon?

Solution. It might seem that it ought to be harder to prove a more general theorem than a less general one, but sometimes not. For example, the more general result might actually be easier because it involves fewer assumptions, and this can help in avoiding the complications of unnecesary hypotheses.

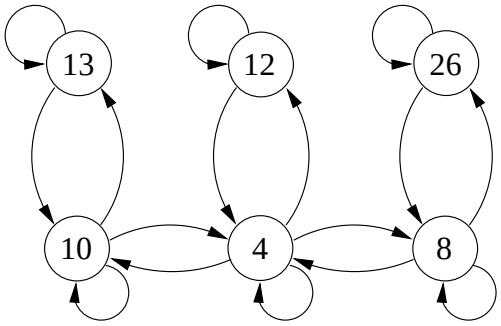
But for an induction proof in particular, using a more general induction hypothesis means we can make a stronger *assumption* in the induction step (namely, we can assume a stronger $P(n)$), which can make it easier to prove the conclusion of the induction step (namely, $P(n+1)$). ■

Solutions to In-Class Problems Week 4, Wed.

Problem 1. Recently MIT students have been taking a hard look at the haphazard building layout, and have been asking some hard questions. As always they know they can use their superior mathematical skills to get some real answers to those hard questions.

They decide to express the MIT building layout as a relation. Let C be the set of all building numbers and let R be the relation on the set C such that $(a, b) \in R$ if building a and building b are physically adjacent and there is a door between a and b (more importantly, one doesn't have to go outside to get from a to b). Note that if $(a, b) \in R$, then (b, a) is also in R, so R is a symmetric relation. For convenience, they also define a building to be related to itself, so $(a, a) \in R$.

(a) For this part only, let C be the set of MIT buildings 10,13,12,4,8,26. Then R looks like this:



- R^2 consists of all pairs of buildings that are connected by traversing exactly 2 edges. Compute R^2.
- $R^{\leq 2}$ consists of all pairs of buildings that are connected by traversing at most 2 edges. Compute $R^{\leq 2}$.
- R^3 consists of all pairs of buildings that are connected by traversing exactly 3 edges. Compute R^3.
- If all self-loops were removed (i.e., all edges of the form (a, a)), would $R^2 = R^{\leq 2}$?

Solution. Since there are self-loops in the connectivity graph (each building is connected to itself), R^2 includes everything which is in R as well. For example, $(13, 10)$ which is in R must also be in

R^2 because you can go from building 13 to building 10 "via 2 edges" by just going around building 13 once and then moving on to building 10. That said, we conclude that

$$R^2 = R \cup \Big\{(13,4),(4,13),(10,12),(12,10),(10,8),(8,10),(12,8),(8,12),(4,26),(26,4)\Big\}$$

$R^{\leq 2} = R^2$.

Similarly, R^3 contains everything which is in R^2 (because of the self-loops), plus all the extra pairs that we get by allowing connections via *three* edges. So we have:

$$R^3 = R^2 \cup \Big\{(13,12),(12,13),(10,26),(26,10),(13,8),(8,13),(26,12),(12,26)\Big\}$$

If the self-loops were removed, R^2 would not contain $(13,13)$ but $R^{\leq 2}$ would. ■

(b) We would like to connect the buildings so that for any pair of buildings (a,b), either one can reach b from a or one can reach a from b. The MIT administration wants to keep the number of connections between buildings as small as possible. In other words, MIT wants the size, $|R|$, of R to be as small as possible. What is the smallest R that will satisfy the MIT students? Is the smallest R unique?

Solution. The smallest graph such that all the buildings are connected would be to connect them in a straight line. The number of edges in that graph is $n-1$. How do we know that this is the smallest number of edges? We will learn a theorem that says that the smallest connected graph with vertices n has at least $n-1$ edges. Each edge contributes two pairs therefore $|R| = 2(n-1)$.

The smallest graph is not unique, for starters we can connect the buildings in a different order in the line. But there are many other connected graphs with n vertices and $n-1$ edges (any tree with n nodes in fact satisfies this constraint, as we shall soon see). ■

Problem 2. **(a)** What are the maxim*al* and minim*al* elements, if any, of the set, $\mathbb{N}$, of all natural numbers under divisibility? Is there a minim*um* or maxim*um* element?

Solution. The minimum (and therefore unique minimal) element is 1 since 1 divides all natural numbers. The maximum (and therefore unique maximal) element is 0 since all numbers divide 0. ■

(b) What are the minimal and maximal elements, if any, of the set of integers ≥ 2 under divisibility?

Solution. All prime numbers are minimal elements, since no numbers divide them. Since there is more than one minimal element, there can't be a minimum element.

There is no maximal element, because for any $n \geq 2$, there is a "larger" number under the divisibility partial order, namely, mn, for any $m > 1$. ■

Problem 3. **(a)** Describe a sequence consisting of the integers from 1 to 10,000 in some order so that there is no increasing or decreasing subsequence of size 101.

Solution.

$$[100 \to 1][200 \to 101][300 \to 201]...[10,000 \to 9901]$$

■

(b) What is the size of the longest chain that is guaranteed to exist in any partially ordered set of n elements? What about the largest antichain?

Solution. Chain size is 1 in the "discrete" partial order in which every two distinct elements are incomparable. Antichain size is 1 if the partial order is total. ■

(c) Describe a partially ordered set that has no minimal or maximal elements.

Solution. $\mathbb{Z}$, $\mathbb{R}$, etc. ■

(d) Describe a partially ordered set that has a *unique minimal* element, but no minimum element.

Solution. $\mathbb{Z} \cup i$ where i is a root of -1, under the usual order $\mathbb{Z}$. So i is incomparable to everything but itself, and is therefore minimal. ■

Problem 4. A pair of 6.042 TAs, Zardosht and Ching, have decided to devote some of their spare time this term to establishing dominion over the entire galaxy. Recognizing this as an ambitious project, they worked out the following table of tasks on the back of Ching's copy of the lecture notes.

1. **Devise a logo** and cool imperial theme music - 8 days.
2. **Build a fleet** of Hyperwarp Stardestroyers out of eating paraphernalia swiped from Lobdell - 18 days.
3. **Seize control** of the United Nations - 9 days, after task #1.
4. **Get shots** for Zardosht's cat, Emilios - 11 days, after task #1.
5. **Open a Starbucks chain** for the army to get their caffeine - 10 days, after task #3
6. **Train an army** of elite interstellar warriors by dragging people to see *The Phantom Menace* dozens of times - 4 days, after tasks #3, #4, and #5.

7. **Launch the fleet** of Stardestroyers, crush all sentient alien species, and establish a Galactic Empire - 6 days, after tasks #2 and #6.

8. **Defeat Microsoft** - 8 days, after tasks #2 and #6.

(a) Express the information in the task list using some type of graph (label the vertices to reflect task lengths).

Solution. The information in the table is represented in the Figure **??** in the form of a directed acyclic graph. Each vertex represents a task, and the weight of a vertex is the completion time. Each directed edge represents a dependency between tasks.

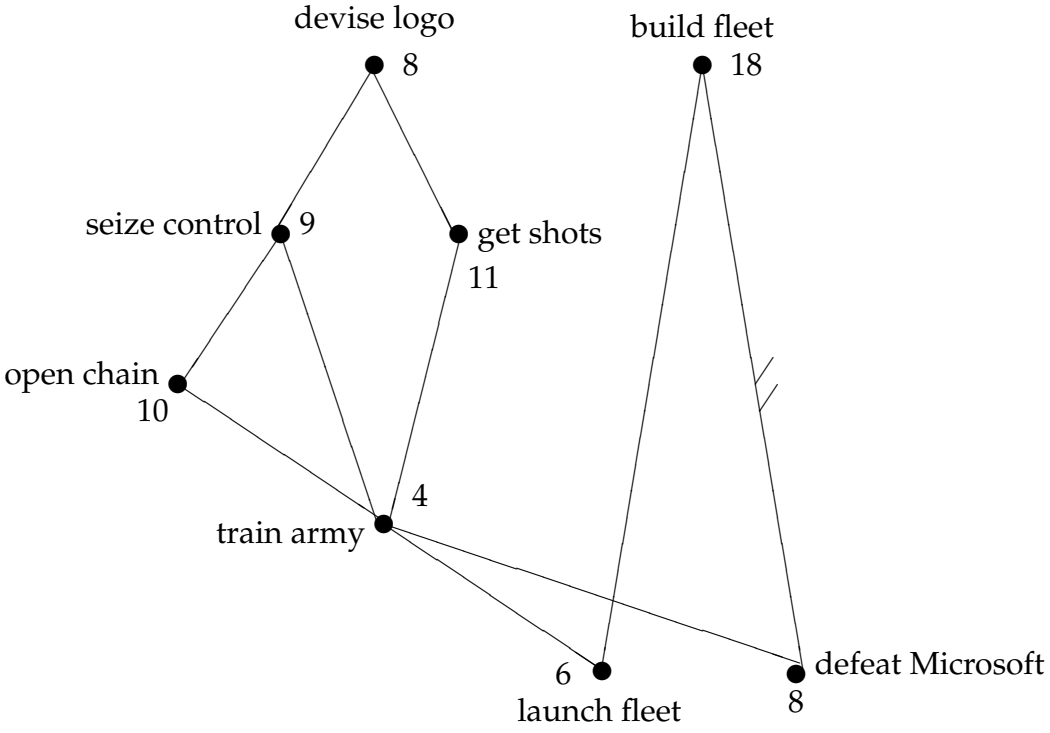


Figure 1: Graph representing the task precedence constraints.

■

(b) Give some valid order in which the tasks might be completed.

Solution. We can easily find several of them. The most natural one is valid, too: #1, #2, #3, #4, #5, #6, #7, #8. ■

Zardosht and Ching want to complete all these tasks in the shortest possible time. However, they have agreed on some constraining work rules.

- Only one person can be assigned to a particular task; they can not work together on a single task.

- Once a person is assigned to a task, that person must work exclusively on the assignment until it is completed. So, for example, Zardosht cannot work on building a fleet for a few days, run get shots for Emilios, and then return to building the fleet.

(c) Zardosht and Ching want to know how long conquering the galaxy will take. Ching suggests dividing the total number of days of work by the number of workers, which is two. What lower bound on the time to conquer the galaxy does this give, and why might the actual time required be greater?

Solution.

$$\frac{8+18+9+11+10+4+6+8}{2} = 37 \text{ days}$$

If working together and interrupting work on a task were permitted, then this answer would be correct. However, the rules may prevent Zardosht and Ching from both working all the time. ■

(d) Zardosht proposes a different method for determining the duration of their project. He suggests looking at the duration of the "critical path", the most time-consuming sequence of tasks such that each depends on the one before. What lower bound does this give, and why might it also be too low?

Solution. The longest sequence of tasks is devising a logo (8 days), seizing the U. N. (9 days), opening a Starbucks (10 days), training the army (4 days), and then defeating Microsoft (8 days). Since these tasks must be done sequentially, galactic conquest will require at least 39 days.

If there were enough workers, this answer would be correct; however, with only two workers, Zardosht and Ching may be unable to make progress on the critical path every day. ■

(e) What is the minimum number of days that Zardosht and Ching need to conquer the galaxy? No proof is required.

Solution. 40 days. Tasks could be divided as follows:

Ching: #1 (days 1-8), #3 (days 9-17), #4 (days 18-28), #8 (days 33-40).

Zardosht: #2 (days 1-18), #5 (days 19-28), #6 (days 29-32), #7 (days 33-38). ■

Appendix

Definition. Let $\preceq$ be a weak (reflexive) partial order on a set, A.

- An element $a \in A$ is a *lower bound* for a subset, $S \subseteq A$ iff $a \preceq s$ for every $s \in S$. Similarly, an element $a \in A$ is an *upper bound* for a subset, $S \subseteq A$ iff $s \preceq a$ for every $s \in S$.
- An element $a \in A$ is the *minimum* element iff a is a lower bound on A. Similarly, an element $a \in A$ is the *maximum* element iff a is an upper bound on A.

- An element $a \in A$ is the *greatest lower bound (glb)* of a subset, $S \subseteq A$ iff a is a lower bound for S, and if $b \in A$ is also a lower bound for S, then $b \preceq a$. Similarly for *least upper bound (lub)*.
- An element $a \in A$ is *minimal* iff there is no element in A that is $\preceq a$ except a itself. Similarly, an element $a \in A$ is *maximal* iff there is no element in A that is $\succeq a$ except a itself.
- Elements $a, b \in A$ are *comparable* iff either $a \preceq b$ or $b \preceq a$. Two elements are *incomparable* iff they are not comparable.
- A subset, $S \subseteq A$ is *totally ordered* iff every two distinct elements in S are comparable.
- A *chain* is a totally ordered subset of A.
- An *antichain* is a subset of A, such that no two elements in it are comparable.

Solutions to In-Class Problems Week 5, Wed.

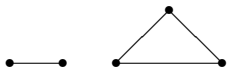
Problem 1. Let L_n be the $(n+1)$-vertex *line graph*, which consists of a single simple path of length n. For example, here is L_4:

The line graph L_4.

A graph is *two-ended* if it has exactly two vertices of degree one and all other vertices have degree two. Note that L_n is a two-ended graph for every $n \geq 1$.

(a) Draw a diagram of the smallest two-ended graph that is *not* isomorphic to a line graph.

Solution. Here is the smallest counterexample:



■

(b) Identify where the following proof makes a logical error (where something is deduced that didn't follow from the previous results and hypotheses).

False Theorem. *Every two-ended graph with n edges is isomorphic to L_n.*

False proof. We prove the thorem by induction on n, the number of edges in the graph, with the hypothesis

$$P(n) ::= \text{ every two-ended graph with } n \text{ edges is isomorphic to } L_n.$$

Base case, $n = 1$: A graph with one edge has the two vertices connected by that edge and some number of vertices not attached to any edge, that is, vertices of degree zero. A two-ended graph cannot have vertices of degree zero, so the only two-ended graph with one edge consists of that edge and the two vertices it joins, which makes it isomorphic to L_1.

Inductive step: Assume that $n \geq 1$, and let G_n be any two-ended graph with n edges. By hypothesis, G_n is isomorphic to L_n.

Now suppose we have a two-ended graph G_{n+1}. We will show that G_{n+1} is also a line graph. Consider how an edge can be added to the line graph G_n to form a two-ended G_{n+1}:

If an edge with two *new* vertices is added to any line graph, the result is not two-ended because it has four degree one vertices. If an edge is attached to one of the degree 2 ("middle") vertices of the line graph, the result is again not two-ended because it has a vertex of degree 3. So the only way to add an edge to the line graph to get a two-ended graph is to have that edge be incident on one side to one of the degree-one vertices —that is, to one end — and to on the other side to a *new* vertex. But adding such an edge to the end of a line graph yields a line graph that is one longer. So the resulting $(n + 1)$-edge graph, G_{n+1}, is indeed isomorphic to L_{n+1}. This proves $P(n + 1)$.

The Theorem follows by induction. □

Solution. The first **logical** error is in the next-to-last sentence: "This proves $P(n+1)$." Something *other than* $P(n + 1)$ was (correctly) proved instead, namely, that every two-ended graph *built by adding an edge* to an n-vertex line graph, is a line graph, L_{n+1}.

But to prove $P(n + 1)$ we had to prove that *every* two-ended graph, G_{n+1}, with $n + 1$ vertices is a line graph. Since not every such G_{n+1} can be built from a line graph by adding an edge (as illustrated in part (a)), the proof did not cover all the possible G_{n+1}'s.

You might want to argue that the proof made a logical error when it began considering "how an edge can be added to the line graph, G_n, to form G_{n+1}," but that's not right. There was no *logical* error at that point. Rather, there was a *strategic* error that lead to the later logical error. A proof could make lots of strategic errors and still wind up being correct, though unduly long-winded, if it eventually got back on track with a correct argument at the end. ■

Problem 2. In this problem you will prove:

Theorem. *A graph G is 2-colorable iff it contains no odd length cycle.*

As usual with "iff" assertions, the proof splits into two proofs: part (a) asks you to prove that the left side of the "iff" implies the right side. The other problem parts prove that the right side implies the left.

(a) Assume the left side and prove the right side. Three to five sentences should suffice.

Solution. First, we assume that G is 2-colorable and prove that G contains no odd length cycle.

Select a 2-coloring of G. Consider an arbitrary cycle with successive vertices $v_1, v_2, \ldots, v_k, v_1$. Then the vertices v_i must be one color for all even i even and the other color for all odd i. (We

could confirm this claim with a proof by induction, but it seems obvious enough to accept without further proof.) Since v_1 and v_k must be colored differently, k must be even. Thus, the cycle has even length. We can make the same argument for any cycle in G, so every cycle has even length.■

(b) Now assume the right side. As a first step toward proving the left side, explain why we can focus on a single connected component H within G.

Solution. Next, we assume that G contains no odd cycle and prove that G is 2-colorable. If we can 2-color every connected component of G, then we can 2-color all of G. Thus, it suffices to show that an arbitrary connected component H of G is 2-colorable. ■

(c) Choose any 2-coloring of a spanning tree, T, of H. Prove that H is 2-colorable by showing that any edge *not* in T must also connect different-colored vertices.

Solution. Any 2-coloring of T can be defined by selecting any fixed vertex v, and coloring a vertex one color if the (unique) path from to it from v has odd length, and coloring it with the other color if the path has even length.

Now let x—y be an edge not T, and consider the unique paths in T. Let z be the last vertex on the path from v to x that also occurs on the path from v to y. Of the paths from z to x and from z to y, exactly one must have odd length; otherwise, these two paths together with the edge x—y would form an odd length cycle.

Now let p be the path from v to z. The v to x path must be p followed by the z to x path, and the v to y path must be p followed by the z to y path. So exactly one of the paths from v to x and from v to y has odd length, which means x and y are colored differently. ■

Problem 3. A portion of a computer program consists of a sequence of calculations where the results are stored in variables, like this:

	Inputs:		a, b
Step 1.	c	$=$	$a + b$
2.	d	$=$	$a * c$
3.	e	$=$	$c + 3$
4.	f	$=$	$c - e$
5.	g	$=$	$a + f$
6.	h	$=$	$f + 1$
	Outputs:		d, g, h

A computer can perform such calculations most quickly if the value of each variable is stored in a *register*, a chunk of very fast memory inside the microprocessor. Computers usually have few

registers, however, so they must be used wisely and reused often. The problem of assigning each variable in a program to a register is called *register allocation*.

In the example above, variables a and b must be assigned different registers, because they hold distinct input values. Furthermore, c and d must be assigned different registers; if they used the same one, then the value of c would be overwritten in the second step and we'd get the wrong answer in the third step. On the other hand, variables b and d may use the same register; after the first step, we no longer need b and can overwrite the register that holds its value. Also, f and h may use the same register; once $f + 1$ is evaluated in the last step, the register holding the value of f can be overwritten.

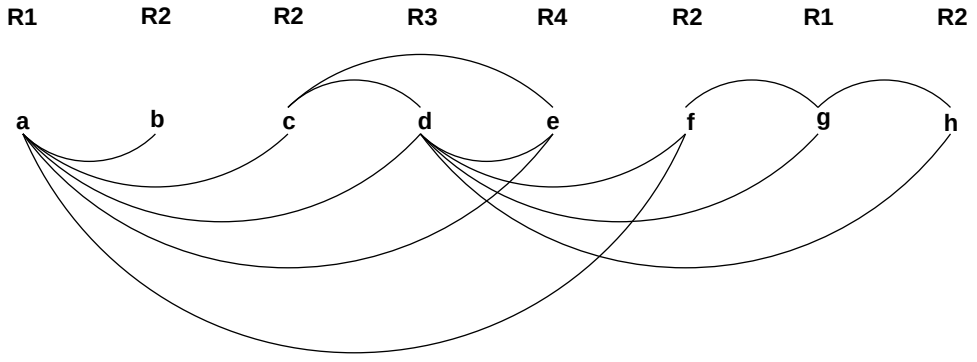
(Assume that the computer carries out each step in the order listed and that each step is completed before the next is begun.)

(a) Recast the register allocation problem as a question about graph coloring. What do the vertices correspond to? Under what conditions should there be an edge between two vertices? Construct the graph corresponding to the example above.

Solution. There is one vertex for each variable. An edge between two vertices indicates that the values of the variables must be stored in different registers.

We can classify each appearance of a variable in the program as either an *assignment* or a *use*. In particular, an appearance is an assignment if the variable is on the left side of an equation or on the "Inputs" line. An appearance of a variable is a use if the variable is on the right side of an equation or on the "Outputs" line.

The *lifetime* of a variable is the segment of code extending from the initial assignment of the variable until the last use. There is an edge between two variables if their lifetimes overlap. This rule generates the following graph:



■

(b) Color your graph using as few colors as you can. Call the computer's registers $R1$, $R2$, etc. Describe the assignment of variables to registers implied by your coloring. How many registers do you need?

Solution. Four registers are needed. One possible assignment of variables to registers is indicated in the figure above.

In general, coloring a graph using the minimum number of colors is quite difficult; no efficient procedure is known. However, the register allocation problem always leads to an *interval graph*. For interval graphs, there are efficient coloring procedures, which can be incorporated into a compiler. ■

(c) Suppose that a variable is assigned a value more than once, as in the code snippet below:

$$\begin{array}{rcl} & \ldots & \\ t & = & r + s \\ u & = & t * 3 \\ t & = & m - k \\ v & = & t + u \\ & \ldots & \end{array}$$

How might you cope with this complication?

Solution. Each time a variable is reassigned, we could regard it as a completely new variable. Then we would regard the example as equivalent to the following:

$$\begin{array}{rcl} & \ldots & \\ t & = & r + s \\ u & = & t * 3 \\ t' & = & m - k \\ v & = & t' + u \\ & \ldots & \end{array}$$

We can now proceed with graph construction and coloring as before. ■

Solutions to In-Class Problems Week 6, Wed.

Problem 1. This problem lets you practice proving simple facts about divisibility.

(a) Prove: If $a \mid b$ and $a \mid c$, then $a \mid sb + tc$ for all s, t.

Solution. Suppose that $a \mid b$ and $a \mid c$. Then there exist integers k_1 and k_2 such that $ak_1 = b$ and $ak_2 = c$. Thus, $sb + tc = s(ak_1) + t(ak_2) = a(sk_1 + tk_2)$, which implies that $a \mid sb + tc$. ■

(b) A number is *perfect* if it is equal to the sum of its positive divisors, other than itself. For example, 6 is perfect, because $6 = 1 + 2 + 3$. Similarly, 28 is perfect, because $28 = 1 + 2 + 4 + 7 + 14$. Explain why $2^{k-1}(2^k - 1)$ is perfect if $2^k - 1$ is prime.

Solution. If $2^k - 1$ is prime, then the only divisors of $2^{k-1}(2^k - 1)$ are:

$$1, \quad 2, \quad 4, \quad \ldots, \quad 2^{k-1}$$

which sum to $2^k - 1$ and

$$1 \cdot (2^k - 1), \quad 2 \cdot (2^k - 1), \quad 4 \cdot (2^k - 1), \quad \ldots, \quad 2^{k-2} \cdot (2^k - 1)$$

which sum to $(2^{k-1} - 1) \cdot (2^k - 1)$. Adding these two sums gives $2^{k-1}(2^k - 1)$, so the number is perfect. ■

Problem 2. Suppose that we have water jugs with capacities a and b. Use induction to prove that the amount of water in each jug is always a linear combination of a and b and at least one jug is either empty or full. Recall that the allowable operations are to fill a jug with water, empty a jug onto the sidewalk, or to transfer water from one jug to another until one the first one is empty or the second one is full.

In Die Hard 6, the water jugs have capacities 3 and 6 gallons, and Bruce must form 4 gallons of water. As a corollary to the above, prove that Bruce dies.

Solution. To prove the first part, we use induction. Let $P(n)$ be the proposition that after n steps, the amount of water in each jug is a linear combination of a and b.

Base case. $P(0)$ is true, because both jugs are initially empty, and $0 \cdot a + 0 \cdot b = 0$.

Inductive step. Now we must show that $P(n)$ implies $P(n+1)$ for $n \geq 0$. So assume that after n steps the amount of water in each jug is a linear combination of a and b. There are two cases:

- If we fill a jug from the fountain or empty a jug into the fountain, then that jug is empty or full. The amount in the other jug remains a linear combination of a and b. So $P(n+1)$ holds.
- Otherwise, we pour water from one jug to another until one is empty or the other is full. By our assumption, the amount in each jug is a linear combination of a and b before we begin pouring:

$$j_1 = s_1 \cdot a + t_1 \cdot b$$
$$j_2 = s_2 \cdot a + t_2 \cdot b$$

  After pouring, one jug is either empty (contains 0 gallons) or full (contains a or b gallons). Thus, the other jug contains either $j_1 + j_2$ gallons, $j_1 + j_2 - a$, or $j_1 + j_2 - b$ gallons, all of which are linear combinations of a and b.

The lemma follows by the principle of induction.

We now show that Bruce dies. The amount in each jug is always of the form $3s + 6t$ by the above lemma. This is always a multiple of 3 by Problem 1.a, so he can not measure out 4 gallons. ■

Problem 3. Prove: Every common divisor of a and b divides $\gcd(a, b)$.

Solution. For some s and t, $\gcd(a, b) = sa + tb$. Let c be a common divisor of a and b. Since $c \mid a$ and $c \mid b$, we know that c divides $sa + tb = \gcd(a, b)$ by part (a) of problem 1. ■

Problem 4. There is a pond. Inside the pond there are n pebbles, arranged in a cycle. A frog is sitting on one of the pebbles. Whenever he jumps, he lands exactly k pebbles away in the clockwise direction, where $0 < k < n$. The frog's meal, a delicious worm, lies on the pebble right next to his, in the clockwise direction.

(a) Describe a situation where the frog can't reach the worm.

Solution. If $k \mid n$ (say $k = 3$ and $n = 6$), then no number of jumps will lead the frog to the worm, as the frog will be returning to his original pebble ad infinitum. ■

(b) In a situation where the frog can actually reach the worm, explain how to use the Pulverizer (see the appendix of this handout for a description of the Pulverizer) to find how many jumps the frog will need.

Solution. Suppose the frog can reach the worm. When he actually reaches it, he has jumped a number of times, say j, and he has travelled around the cycle a number of times, call it c. Then, the distance that the frog has covered is both $j \cdot k$ and $c \cdot n + 1$, so that

$$jk = cn + 1.$$

But this means that 1 can be written as a *linear combination* of n and k:

$$(-c)n + jk = 1.$$

Since 1 is positive, we conclude that it is a *positive linear combination* of n and k. And since it is the smallest positive integer, we also conclude that it is the *smallest positive linear combination* of n and k. But we have seen in lecture that the smallest positive linear combination of two integers is their GCD. So, the GCD of n and k is 1:

$$\gcd(n, k) = 1$$

and we can use the Pulverizer to find $-c$ and j. ■

(c) Compute the number of jumps if $n = 50$ and $k = 21$. Anything strange?

Solution. We go through the steps as described in the appendix to get that $1 = 8 \cdot 50 - 19 \cdot 21$, or $1 = -(-8) \cdot 50 + (-19) \cdot 21$. Hence, $c = -8$ and $j = -19$, which makes little sense. What does it mean for the frog to make -19 jumps?

The point is that the Pulverizer is guaranteed to give us the integers coefficients of a linear combination that equals the GCD, but it promises nothing about the signs of those coefficients —which, in this case we wanted them to be $-$ and $+$. To get coefficients of the desired sign, we have to think more.

So, we know $1 = 8 \cdot 50 - 19 \cdot 21$. Or, to obtain meaningful signs for the numbers, $19 \cdot 21 = 8 \cdot 50 - 1$. That is, after 19 jumps the frog will have covered 8 full cycles but 1 pebble. So, he will be right next to his original pebble, but in the counter-clockwise direction. Given this, how can he reach the pebble he is after?

Well, if he makes 19 more jumps, he will land 2 pebbles away from his original position in the counter-clockwise direction. Another 19 jumps will lead him 3 pebbles away, and so on. After a total of 49 sets of 19 jumps, he will be 49 pebbles away from its original position in the counter-clockwise direction, which is of course the worm's pebble. Then, the frog will have made $49 * 19 = 931$ jumps.

Here is the table produced by the Pulverizer:

x	y	$(x \text{ rem } y)$	$=$	$x - q \cdot y$
50	21	8	$=$	$50 - 2 \cdot 21$
21	8	5	$=$	$21 - 2 \cdot 8$
			$=$	$21 - 2 \cdot (50 - 2 \cdot 21)$
			$=$	$-2 \cdot 50 + 5 \cdot 21$
8	5	3	$=$	$8 - 1 \cdot 5$
			$=$	$(50 - 2 \cdot 21) - 1 \cdot (-2 \cdot 50 + 5 \cdot 21)$
			$=$	$3 \cdot 50 - 7 \cdot 21$
5	3	2	$=$	$5 - 1 \cdot 3$
			$=$	$(-2 \cdot 50 + 5 \cdot 21) - 1 \cdot (3 \cdot 50 - 7 \cdot 21)$
			$=$	$-5 \cdot 50 + 12 \cdot 21$
3	2	1	$=$	$3 - 1 \cdot 2$
			$=$	$(3 \cdot 50 - 7 \cdot 21) - 1 \cdot (-5 \cdot 50 + 12 \cdot 21)$
			$=$	$\boxed{8 \cdot 50 - 19 \cdot 21}$
2	1	0		

■

A Appendix: The Pulverizer

Euclid's algorithm for finding the GCD of two numbers relies on repeated application of the equation:

$$\gcd(a, b) = \gcd(b, a \text{ rem } b)$$

For example, we can compute the GCD of 259 and 70 as follows:

$$\begin{aligned} \gcd(259, 70) &= \gcd(70, 49) && \text{since } 259 \text{ rem } 70 = 49 \\ &= \gcd(49, 21) && \text{since } 70 \text{ rem } 49 = 21 \\ &= \gcd(21, 7) && \text{since } 49 \text{ rem } 21 = 7 \\ &= \gcd(7, 0) && \text{since } 21 \text{ rem } 7 = 0 \\ &= 7. \end{aligned}$$

The Pulverizer goes through the same steps, but requires some extra bookkeeping along the way: as we compute $\gcd(a, b)$, we keep track of how to write each of the remainders (49, 21, and 7, in the example) as a linear combination of a and b (this is worthwhile, because our objective is to write the last nonzero remainder, which is the GCD, as such a linear combination). For our example, here is this extra bookkeeping:

x	y	$(x \text{ rem } y)$	$=$	$x - q \cdot y$
259	70	49	$=$	$259 - 3 \cdot 70$
70	49	21	$=$	$70 - 1 \cdot 49$
			$=$	$70 - 1 \cdot (259 - 3 \cdot 70)$
			$=$	$-1 \cdot 259 + 4 \cdot 70$
49	21	7	$=$	$49 - 2 \cdot 21$
			$=$	$(259 - 3 \cdot 70) - 2 \cdot (-1 \cdot 259 + 4 \cdot 70)$
			$=$	$\boxed{3 \cdot 259 - 11 \cdot 70}$
21	7	0		

We began by initializing two variables, $x = a$ and $y = b$. In the first two columns above, we carried out Euclid's algorithm. At each step, we computed x rem y, which can be written in the form $x - q \cdot y$. (Remember that the Division Algorithm says $x = q \cdot y + r$, where r is the remainder. We get $r = x - q \cdot y$ by rearranging terms.) Then we replaced x and y in this equation with equivalent linear combinations of a and b, which we already had computed. After simplifying, we were left with a linear combination of a and b that was equal to the remainder as desired. The final solution is boxed.

Solutions to In-Class Problems Week 7, Wed.

Problem 1. Let's try out RSA! There is a complete description of the algorithm at the bottom of the page. You'll probably need extra paper. *Check your work carefully!*

(a) As a team, go through the **beforehand** steps.

- Choose primes p and q to be relatively small, say in the range 10-40. In practice, p and q might contain several hundred digits, but small numbers are easier to handle with pencil and paper.
- Try $e = 3, 5, 7, \ldots$ until you find something that works. Use Euclid's algorithm to compute the gcd.
- Find d using the Pulverizer (see appendix for a reminder on how the Pulverizer works).

When you're done, put your public key on the board. This lets another team send you a message.

(b) Now send an encrypted message to another team using their public key. Select your message m from the codebook below:

- 2 = Greetings and salutations!
- 3 = Yo, wassup?
- 4 = You guys are slow!
- 5 = All your base are belong to us.
- 6 = Someone on *our* team thinks someone on *your* team is kinda cute.
- 7 = You *are* the weakest link. Goodbye.

(c) Decrypt the message sent to you and verify that you received what the other team sent!

(d) Explain how you could read messages encrypted with RSA if you could quickly factor large numbers.

Solution. Suppose you see a public key (e, n). If you can factor n to obtain p and q, then you can compute d using the Pulverizer. This gives you the secret key (d, n), and so you can decode messages as well as the intended recipient. ■

RSA Public Key Encryption

Beforehand The receiver creates a public key and a secret key as follows.

1. Generate two distinct primes, p and q.
2. Let $n = pq$.
3. Select an integer e such that $\gcd(e, (p-1)(q-1)) = 1$.
   The *public key* is the pair (e, n). This should be distributed widely.
4. Compute d such that $de \equiv 1 \pmod{(p-1)(q-1)}$.
   The *secret key* is the pair (d, n). This should be kept hidden!

Encoding The sender encrypts message m to produce m' using the public key:

$$m' = m^e \text{ rem } n.$$

Decoding The receiver decrypts message m' back to message m using the secret key:

$$m = (m')^d \text{ rem } n.$$

Problem 2. A critical question is whether decrypting an encrypted message always gives back the original message! Mathematically, this amounts to asking whether:

$$m^{de} \equiv m \pmod{pq}.$$

Note that the procedure ensures that $de = 1 + k(p-1)(q-1)$ for some integer k.

(a) Use Euler's Theorem to prove that $m^{de} \equiv m \pmod{pq}$ for all messages m relatively prime to pq. (Euler's Theorem says that if k is relatively prime to n then $k^{\phi(n)} \equiv 1 \pmod{n}$.) In practice, is m likely to be relatively prime to pq or not?

Solution.

$$\begin{aligned} m^{de} &\equiv m^{1+k\phi(pq)} \pmod{pq} \\ &\equiv m \cdot (m^{\phi(pq)})^k \pmod{pq} \\ &\equiv m \cdot 1^k \pmod{pq} \end{aligned}$$

The first step uses the fact that $\phi(pq) = (p-1)(q-1)$, the second uses exponent laws, and third uses Euler's Theorem. If p and q are hundred-digit primes, m is very likely to be relatively prime to both p and q. ■

(b) This congruence actually holds for all messages m. First, use Fermat's theorem to prove that $m \equiv m^{de} \pmod{p}$ for all m. (Fermat's Theorem says that $a^{p-1} \equiv 1 \pmod{p}$ if p is a prime that does not divide a.)

Solution. If m is a multiple of p, then the claim holds because both sides are congruent to 0 mod p. Otherwise, suppose that m is not a multiple of p. Then:

$$\begin{aligned} m^{1+k(p-1)(q-1)} &\equiv m \cdot (m^{p-1})^{k(q-1)} \pmod{p} \\ &\equiv m \cdot 1^{k(q-1)} \pmod{p} \\ &\equiv m \pmod{p} \end{aligned}$$

The second step uses Fermat's theorem, which says that $m^{p-1} \equiv 1 \pmod{p}$ provided m is not a multiple of p. ■

(c) By the same argument, you can equally well show that $m \equiv m^{ed} \pmod{q}$. Show that these two facts together imply that $m \equiv m^{ed} \pmod{pq}$ for all m.

Solution. We know that:

$$\begin{aligned} p \mid (m - m^{ed}), \\ q \mid (m - m^{ed}). \end{aligned}$$

Thus, both p and q appear in the prime factorization of $m - m^{ed}$. Therefore, $pq \mid (m - m^{ed})$, and so:

$$m \equiv m^{ed} \pmod{pq}.$$

■

1 Appendix: The Pulverizer

Euclid's algorithm for finding the GCD of two numbers relies on repeated application of the equation:

$$\gcd(a, b) = \gcd(b, a \text{ rem } b)$$

For example, we can compute the GCD of 259 and 70 as follows:

$$\begin{aligned} \gcd(259, 70) &= \gcd(70, 49) && \text{since } 259 \text{ rem } 70 = 49 \\ &= \gcd(49, 21) && \text{since } 70 \text{ rem } 49 = 21 \\ &= \gcd(21, 7) && \text{since } 49 \text{ rem } 21 = 7 \\ &= \gcd(7, 0) && \text{since } 21 \text{ rem } 7 = 0 \\ &= 7. \end{aligned}$$

The Pulverizer goes through the same steps, but requires some extra bookkeeping along the way: as we compute $\gcd(a, b)$, we keep track of how to write each of the remainders (49, 21, and 7, in the example) as a linear combination of a and b (this is worthwhile, because our objective is to write the last nonzero remainder, which is the GCD, as such a linear combination). For our example, here is this extra bookkeeping:

x	y	$(x \text{ rem } y)$	$=$	$x - q \cdot y$
259	70	49	$=$	$259 - 3 \cdot 70$
70	49	21	$=$	$70 - 1 \cdot 49$
			$=$	$70 - 1 \cdot (259 - 3 \cdot 70)$
			$=$	$-1 \cdot 259 + 4 \cdot 70$
49	21	7	$=$	$49 - 2 \cdot 21$
			$=$	$(259 - 3 \cdot 70) - 2 \cdot (-1 \cdot 259 + 4 \cdot 70)$
			$=$	$\boxed{3 \cdot 259 - 11 \cdot 70}$
21	7	0		

We began by initializing two variables, $x = a$ and $y = b$. In the first two columns above, we carried out Euclid's algorithm. At each step, we computed x rem y, which can be written in the form $x - q \cdot y$. (Remember that the Division Algorithm says $x = q \cdot y + r$, where r is the remainder. We get $r = x - q \cdot y$ by rearranging terms.) Then we replaced x and y in this equation with equivalent linear combinations of a and b, which we already had computed. After simplifying, we were left with a linear combination of a and b that was equal to the remainder as desired. The final solution is boxed.

Solutions to In-Class Problems Week 8, Wed.

Problem 1. We begin with two large glasses. The first glass contains a pint of water, and the second contains a pint of wine. We pour $1/3$ of a pint from the first glass into the second, stir up the wine/water mixture in the second glass, and then pour $1/3$ of a pint of the mix back into the first glass and repeat this pouring back-and-forth process a total of n times.

(a) Describe a closed form formula for the amount of wine in the first glass after n back-and-forth pourings.

Solution. The state of the system of glasses/wine/water at the beginning of a round of pouring and pouring back is determined by the total amount of wine in the first glass. Suppose at the beginning of some round, the first glass contains w pints of wine, $0 \leq w \leq 1$ and $1 - w$ pints of water. The second glass contains the rest of the wine and water.

Pouring $1/3$ pint from first glass to second leaves $2/3$ pints of liquid and $(2/3)w$ wine in the first glass, and $4/3$ pints of liquid and $1 - (2/3)w$ wine in the second glass. Pouring $1/3$ pint back from second into first transfers a proportion of $(1/3)/(4/3)$ of the wine in the second glass into the first. So the round completes with both glasses containing a pint of liquid, and the first glass containing

$$(2/3)w + (1/4)(1 - (2/3)w) = 1/4 + w/2$$

pints of wine. After one more round, the first glass contains

$$1/4 + (1/4 + w/2)/2 = 1/4 + 1/8 + w/2^2$$

pints of wine, and after n more rounds

$$\begin{aligned} w/2^n + \Sigma_{i=1}^{n}(1/2)^{i+1} &= w/2^n + (1/2)\Sigma_{i=1}^{n}(1/2)^i \\ &= w/2^n + (1/2)(-1 + \Sigma_{i=0}^{n}(1/2)^i) \\ &= w/2^n + (1/2)(-1 + (1 - (1/2)^{n+1})/(1 - 1/2)) \\ &= w/2^n - 1/2 + 1 - (1/2)^{n+1} \\ &= w/2^n + 1/2 - (1/2)^{n+1}. \end{aligned}$$

Since $w = 0$ initially, the pints of wine in the first glass after n rounds is

$$1/2 - (1/2)^{n+1}.$$

■

(b) What is the limit of the amount of wine in each glass as n approaches infinity?

Solution. The limiting amount of wine in the first glass approaches $1/2$ from below as n approaches infinity. In fact, it approaches $1/2$ no matter how the wine was initially distributed. This of course is what you would expect: after a thorough mixing the glasses should contain essentially the same amount of wine. ■

Problem 2. Suppose you were about to enter college today and a college loan officer offered you the following deal: \$25,000 at the start of each year for four years to pay for your college tuition and an option of choosing one of the following repayment plans:

Plan A: Wait four years, then repay \$20,000 at the start of each year for the next ten years.

Plan B: Wait five years, then repay \$30,000 at the start of each year for the next five years.

Suppose the annual interest rate paid by banks is 7% and does not change in the future.

(a) Assuming that it's no hardship for you to meet the terms of either payback plan, which one is a better deal? (You will need a calculator.)

Solution. \$1 today will be worth $\$1.07$ next year, and $\$1.07^2$ the year after, *etc*. So set $r = \frac{1}{1.07}$. Then:

$$\begin{aligned}
&\text{current value of Plan A} \\
&= \sum_{y=4}^{13} 20000 \cdot r^y \\
&= \sum_{y=0}^{9} 20000 \cdot r^{y+4} \\
&= r^4 \cdot \sum_{y=0}^{9} 20000 \cdot r^y \\
&= 20000r^4 \cdot \sum_{y=0}^{9} r^y \\
&= 20000r^4 \cdot \frac{1-r^{10}}{1-r} \\
&= \$114,66.69
\end{aligned}$$

$$\begin{aligned}
&\text{current value of Plan B}\\
&= \sum_{y=5}^{9} 30000 \cdot r^y\\
&= \sum_{y=0}^{4} 30000 \cdot r^{y+5}\\
&= r^5 \cdot \sum_{y=0}^{4} 30000 \cdot r^y\\
&= 30000r^5 \cdot \sum_{y=0}^{4} r^y\\
&= 30000r^5 \cdot \frac{1-r^5}{1-r}\\
&= \$93,840.63
\end{aligned}$$

You should clearly take Plan B. You will be paying back much less in today's dollars. ■

(b) What is the loan officer's effective profit (in today's dollars) on the loan?

Solution. The value of the money you are given is:

$$\begin{aligned}
Loan &= \sum_{y=0}^{3} 25000 \cdot r^y\\
&= 25000 \cdot \sum_{y=0}^{3} r^y\\
&= 25000 \cdot \frac{1-r^4}{1-r}\\
&= \$90,607.90
\end{aligned}$$

Therefore, the loan officer's profit is effectively $\$3,233$. (Or $\$24,059$ if we are not on the ball). ■

Problem 3. Riemann's Zeta Function $\zeta(k)$ is defined to be the infinite summation:

$$1 + \frac{1}{2^k} + \frac{1}{3^k} \cdots = \sum_{j \geq 1} \frac{1}{j^k}$$

Below is a proof that

$$\sum_{k \geq 2} (\zeta(k) - 1) = 1$$

Justify each line of the proof. (P.S. The purpose of this exercise is to highlight some of the rules for manipulating series. Don't worry about the significance of this identity.)

$$\begin{aligned}
\sum_{k\geq 2}(\zeta(k)-1) &= \sum_{k\geq 2}\left[\left(\sum_{j\geq 1}\frac{1}{j^k}\right)-1\right] && (1)\\
&= \sum_{k\geq 2}\sum_{j\geq 2}\frac{1}{j^k} && (2)\\
&= \sum_{j\geq 2}\sum_{k\geq 2}\frac{1}{j^k} && (3)\\
&= \sum_{j\geq 2}\frac{1}{j^2}\sum_{k\geq 0}\frac{1}{j^k} && (4)\\
&= \sum_{j\geq 2}\frac{1}{j^2}\cdot\frac{1}{1-1/j} && (5)\\
&= \sum_{j\geq 2}\frac{1}{j(j-1)} && (6)\\
&= \lim_{n\to\infty}\sum_{j=2}^{n}\frac{1}{j(j-1)} && (7)\\
&= \lim_{n\to\infty}\sum_{j=2}^{n}\frac{1}{j-1}-\frac{1}{j} && (8)\\
&= \lim_{n\to\infty}(1-\frac{1}{n}) && (9)\\
&= 1 && (10)
\end{aligned}$$

Solution. (1) Definition of $\zeta(k)$.

(2) Because $\sum_{j\geq 1}\frac{1}{j^k} = 1+\sum_{j\geq 2}\frac{1}{j^k}$.

(3) Reordering; this is ok because at this point all terms are positive.

(4) Because $\sum_{k\geq 2}\frac{1}{j^k} = \sum_{k\geq 0}\frac{1}{j^{k+2}} = \sum_{k\geq 0}\frac{1}{j^k\cdot j^2} = \frac{1}{j^2}\sum_{k\geq 0}\frac{1}{j^k}$.

(5) Sum of a geometric series.

(6) Algebra inside every summand.

(7) Definition of infinite summation.

(8) Algebra inside every summand.

(9) The sum telescopes: 1 is added once; every one of $\frac{1}{2}, \frac{1}{3}, \ldots, \frac{1}{n-1}$ is subtracted once and then added once; $\frac{1}{n}$ is subtracted once.

(10) Simple limits. ■

Solutions to In-Class Problems Week 9, Wed.

Problem 1. A license plate consists of either:

- 3 letters followed by 3 digits (standard plate)
- 5 letters (vanity plate)
- 2 characters – letters or numbers (big shot plate)

Let L be the set of all possible license plates.

(a) Express L in terms of

$$\mathcal{A} = \{A, B, C, \ldots, Z\}$$
$$\mathcal{D} = \{0, 1, 2, \ldots, 9\}$$

using unions ($\cup$) and set products ($\times$).

Solution.

$$L = (A^3 \times D^3) \cup A^5 \cup (A \cup D)^2$$

■

(b) Compute $|L|$, the number of different license plates, using the sum and product rules.

Solution.

$$\begin{aligned}
|L| &= \left|(A^3 \times D^3) \cup A^5 \cup (A \cup D)^2\right| \\
&= \left|(A^3 \times D^3)\right| + \left|A^5\right| + \left|(A \cup D)^2\right| && \text{Sum Rule} \\
&= |A|^3 \cdot |D|^3 + |A|^5 && |A \cup D|^2 \text{Product Rule} \\
&= |A|^3 \cdot |D|^3 + |A|^5 && (|A| + |D|)^2 \text{Sum Rule} \\
&= 26^3 \cdot 10^3 + 26^5 + 36^2 = 29458672
\end{aligned}$$

■

Problem 2. Let p be a prime and k a positive integer.

(a) How many positive integers less than p^k are divisible by p?

Solution. Every pth integer is divisible by p, namely $p, 2p, 3p, \ldots (p^{k-1} - 1)p$, so the answer is $p^{k-1} - 1$. ■

(b) What is the value, $\phi(p^k)$, of the Euler function at p^k?

Solution. There are $p^k - 1$ positive integers less than p^k, of which $p^{k-1} - 1$ are divisible by p by part (a), and $\phi(p^k)$ are relatively prime to p^k by definition of Euler's function. But a number is relatively prime to p^k iff it is not divisible by p, so

$$(p^{k-1} - 1) + \phi(p^k) = p^k - 1$$

by the Sum Rule. Therefore,

$$\phi(p^k) = p^k - p^{k-1}.$$

■

Problem 3. For each part below, describe a bijection between the two sets mentioned. The existence of such a bijection proves that the two sets are the same size.

A good approach is to describe an element of the first set using variables and then describe the corresponding element of the second set in terms of those variables. For example, we might describe a bijecton from ways of selecting a dozen doughnuts from five varieties to a 16-bit string with four 1's as follows:

Map a dozen doughnuts consisting of:

$$c \text{ chocolate, } l \text{ lemon-filled, } s \text{ sugar, } g \text{ glazed, and } p \text{ plain}$$

to the sequence:

$$\underbrace{0\ldots0}_{c}\ 1\ \underbrace{0\ldots0}_{l}\ 1\ \underbrace{0\ldots0}_{s}\ 1\ \underbrace{0\ldots0}_{g}\ 1\ \underbrace{0\ldots0}_{p}$$

Everyone in your group should write out complete answers— you'll all benefit from the practice!

(a) Describe a bijection between the set of 30-bit sequences with 10 zeros and 20 ones and paths from $(0, 0)$ to $(10, 20)$ consisting of right-steps (which increment the first coordinate) and up-steps (which increment the second coordinate).

Solution. Map the 30-bit sequence $b_1 b_2 \ldots b_{30}$ to a path where the i-th step is right if $b_i = 0$ and up if $b_i = 1$. ■

(b) Find a bijection between the set of n-bit sequences and the set of all subsets of $\{x_1, x_2, \ldots, x_n\}$.

Solution. Map the n-bit sequence $b_1 b_2 \ldots b_n$ to a subset that contains x_i if and only if $b_i = 1$. ■

(c) Mr. and Mrs. Grumperson have collected 13 identical pieces of coal as Christmas presents for their beloved children, Lucy and Spud. Describe a bijection between the set of all ways of distributing the 13 coal pieces to the two children and the set of 14-bit sequences with exactly 1 one.

Solution. Map a distribution in which Lucy get l pieces and Spud gets s pieces to a 14-bit sequence with l zeros, a one, and then s zeros. ■

(d) On Christmas Eve, Mr. and Mrs. Grumperson remember that they have a third child, little Bottlecap, locked in the attic. Describe a bijection between the set of all ways of distributing the 13 coal pieces to the three children and the set of 15-bit sequences with exactly 2 ones.

Solution. Map a distribution in which Lucy gets l pieces, Spud gets s pieces, and Bottlecap gets b pieces to a 15-bit sequence with l zeros, a one, s zeros, a one, and b zeros. ■

(e) On reflection, Mr. and Mrs. Grumperson decide that each of their three children should receive *at least two* pieces of coal for Christmas. Describe a bijection between the set of all ways of distributing the 13 coal pieces to the three Grumperson children given this constraint and the set of 9-bit sequences with exactly 2 ones.

Solution. Map a distribution in which Lucy gets $l \geq 2$ pieces, Spud gets $s \geq 2$ pieces, and Bottlecap gets $b \geq 2$ pieces to a 9-bit sequence with exactly $l - 2$ zeros, a one, $s - 2$ zeros, a one, and $b - 2$ zeros. ■

(f) Describe a bijection between the set of 110-bit sequences with exactly 10 ones and solutions over the natural numbers to the equation:

$$x_1 + x_2 + \cdots + x_{10} \quad \leq \quad 100$$

Solution. Let x_1 be the number of zeros before the first 1, x_2, be the number of zeros between the first and second 1, etc. Note that zeros after the tenth 1 do not contribute to the value of any of the variables $x_1, \ldots, x_{10}$; this allows us to count solutions to the inequality (≤ 100) rather than the equality ($= 100$). ■

(g) Describe a bijection between solutions to the inequality in the preceding problem part and sequences $(y_1, y_2, \ldots, y_{10})$ such that:

$$0 \leq y_1 \leq y_2 \leq \cdots \leq y_{10} \leq 100$$

Solution. Let $y_i = x_1 + \cdots + x_i$ for each i from 1 to 10. ■

Problem 4. A *numbered tree* is a tree whose vertex set is $\{1, 2, \ldots, n\}$ for some $n \geq 2$. We define the *code* of the numbered tree to be a sequence of $n-2$ integers from 1 to n obtained by the following recursive process:

> If $n = 2$, stop—the code is the empty sequence. Otherwise, write down the *father* of the largest leaf[1], delete this *leaf*, and continue the process on the resulting smaller tree.

For example, the codes of a couple of numbered trees are shown in the Figure 1.

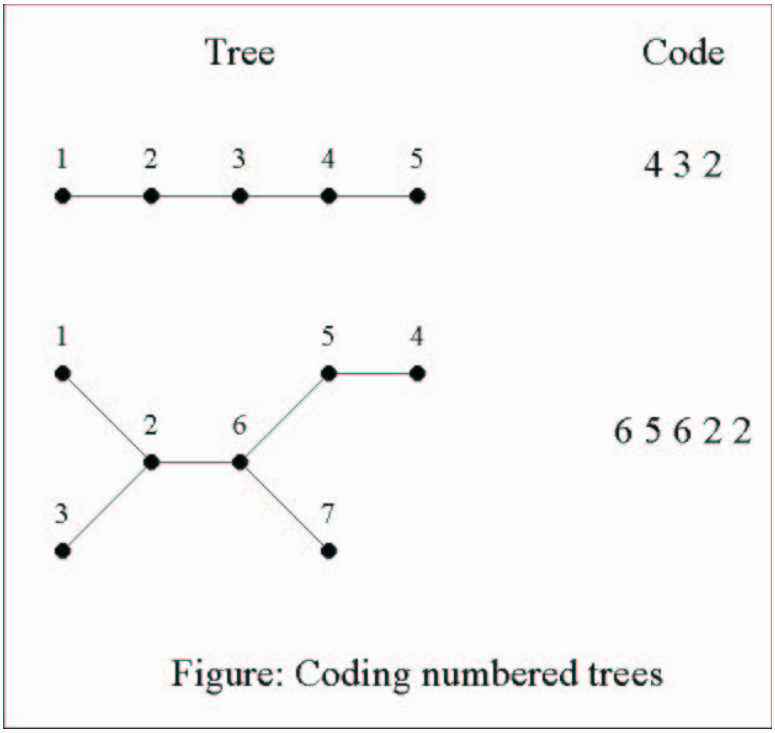


Figure 1:

(a) Describe a procedure for reconstructing a numbered tree from its code.

Solution. The key observation is that, given a code of length $n-2$, the numbers between 1 and n which *do not appear* in the code must be leaves of the tree. Hence, the largest missing number is a leaf attached to the first number of the code. The rest of the tree can now be reconstructed by deleting the first number in the code, henceforth ignoring the largest leaf, and proceeding

[1]The necessarily unique node adjacent to a leaf is called its *father*

recursively on the rest of the code. (We're using the obvious fact that what's left after deleting a leaf from a tree is another tree.)

More precisely, the reconstruction procedure applies to any finite tree whose vertex set is totally ordered. The procedure takes *two* parameters: the vertex set, V, and a length $|V| - 2$ "code" sequence, S, of elements in V. If l is the largest element in V which does not appear in S, and f is the first element of S, then the reconstructed tree is obtained by adding edge (l, f) to the tree reconstructed by calling the procedure recursively with first argument $V - \{l\}$ and second argument equal to the code obtained by erasing the initial f from S. The procedure terminates when $|V| = 2$, returning the edge between the two numbers in V.

To justify the key observation, note that any vertex that gets deleted by the process and was not a leaf to begin with, must have been the father of a previously deleted leaf, which means it would appear in the code. So the missing integers must have been leaves to begin with or must be one of the two undeleted vertices left when the coding process terminates. But by the end of the process the two remaining vertices are leaves, and if they weren't leaves to begin with, they must have become leaves by having their sons deleted, which means they would not have been missing from the code. So the two vertices remaining at the end must also have been leaves of the original tree. ■

(b) How many numbered trees with n vertices are there? Justify your answer assuming the result of the previous problem part.

Solution. There are exactly as many n-vertex numbered trees as the number of possible code words, that is, the number of length $n - 2$ sequences integers between 1 and n. So there are n^{n-2} numbered trees.

The reason is that the map from trees to codes is a bijection. To see this, note that the tree reconstruction procedure finds *the only possible tree* with that code. So there can't be two trees with the same code, i.e., the map from a tree to its code is an injection. But since the reconstruction procedure finds a tree for every possible codeword, the map from trees to codes is also a surjection. ■

Solutions to In-Class Problems Week 10, Wed.

Problem 1. Find the coefficients of

(a) x^5 in $(1+x)^{11}$

Solution.

$$\binom{11}{5} = 462$$

■

(b) x^8y^9 in $(3x+2y)^{17}$

Solution.

$$\binom{17}{8}3^8 2^9$$

■

(c) a^6b^6 in $(a^2+b^3)^5$

Solution. $a^6b^6 = (a^2)^3(b^3)^2$, so the coefficient is

$$\binom{5}{3} = 10$$

■

Problem 2. According to the Multinomial theorem, $(w+x+y+z)^n$ can be expressed as a sum of terms of the form

$$\binom{n}{r_1, r_2, r_3, r_4} w^{r_1}x^{r_2}y^{r_3}z^{r_4}.$$

How many terms are there in the sum?

Solution. The sum is over all 4-tuples of nonnegative integers (r_1, r_2, r_3, r_4) such that

$$r_1 + r_2 + r_3 + r_4 = n.$$

We know this is the same as the number of binary words with n zeroes and 3 ones, namely

$$\binom{n+3}{3}.$$

■

Combinatorial proofs of identities

Recall the basic plan for a combinatorial proof of an identity $x = y$:

1. Define a set S.
2. Show that $|S| = x$ by counting one way.
3. Show that $|S| = y$ by counting another way.
4. Conclude that $x = y$.

Problem 3. You want to choose a team of m people from a pool of n people for your startup company, and from these m people you want to choose k to be the team managers. You took 6.042, so you know you can do this in

$$\binom{n}{m}\binom{m}{k}$$

ways. But your CFO, who went to Harvard Business School, comes up with the formula

$$\binom{n}{k}\binom{n-k}{m-k}.$$

Before doing the reasonable thing —dump on your CFO or Harvard Business School— you decide to check his answer against yours.

(a) Start by giving an *algebraic proof* that your CFO's formula agrees with yours.

Solution.

$$\begin{aligned}
\binom{n}{m}\binom{m}{k} &= \frac{n!}{m!(n-m)!}\frac{m!}{k!(m-k)!} \\
&= \frac{n!}{(n-m)!k!(m-k)!} \\
&= \frac{n!(n-k)!}{(n-m)!k!(m-k)!(n-k)!} \\
&= \frac{n!}{k!(n-k)!}\frac{(n-k)!}{(n-m)!(m-k)!} \\
&= \frac{n!}{k!(n-k)!}\frac{(n-k)!}{((n-k)-(m-k))!(m-k)!} \\
&= \binom{n}{k}\binom{n-k}{m-k}.
\end{aligned}$$

■

(b) Now give a *combinatorial argument* proving this same fact.

Solution. Instead of choosing first m from n and then k from m, you could alternately choose the k managers from the n people and then choose $m-k$ people to fill out the team from the remaining $n-k$ people. This gives you $\binom{n}{k}\binom{n-k}{m-k}$ ways of picking your team. Since you must have the same number of options regardless of the order in which you choose to pick team members and managers,

$$\binom{n}{m}\binom{m}{k} = \binom{n}{k}\binom{n-k}{m-k}.$$

■

Problem 4. Now give a combinatorial proof of the following, more interesting theorem:

$$n2^{n-1} = \sum_{k=1}^{n} k\binom{n}{k}$$

Hint: Let S be the set of all length-n sequences of 0's, 1's and a single *.

Solution. Let $P ::= \{0,\ldots,n-1\} \times \{0,1\}^{n-1}$. On the one hand, there is a bijection from P to S by mapping (k,x) to the word obtained by inserting a * just after the kth bit in the length-$n-1$ binary word, x. So

$$|S| = |P| = n2^{n-1} \tag{1}$$

by the Product Rule.

On the other hand, every sequence in S contains between 1 and n nonzero entries since the $*$, at least, is nonzero. The mapping from a sequence in S with exactly k nonzero entries to a pair consisting of the set of positions of the nonzero entries and the position of the * among these entries is a bijection, and the number of such pairs is $\binom{n}{k}k$ by the Generalized Product Rule. Thus, by the Sum Rule:

$$|S| = \sum_{k=1}^{n} k\binom{n}{k}$$

Equating this expression and the expression (1) for $|S|$ proves the theorem. ■

Learning to count takes practice! The following problems offer some.

Problem 5. A pizza house is having a promotional sale. Their commercial reads:

> We offer 9 different toppings for your pizza! Buy 3 large pizzas at the regular price, and you can get each one with as many different toppings as you wish, absolutely free. That's $22,369,621$ different ways to choose your pizzas!

The ad writer was a former Harvard student who had evaluated the formula $(2^9)^3/3!$ on his calculator and gotten close to $22,369,621$. Unfortunately, $(2^9)^3/3!$ is obviously not an integer, so clearly something is wrong. What mistaken reasoning might have led the ad writer to this formula? Explain how to fix the mistake and get a correct formula.

Solution. The number of ways to choose toppings for one pizza is the number of the possible subsets of the set of 9 toppings, namely, 2^9. The ad writer presumably then used the Product Rule to conclude that there were $(2^9)^3$ *sequences* of three topping choices. Then he probably reasoned that each way of making three topping choices arises from 3! sequences, so the Division Rule would imply that the number of ways to choose three pizzas is $(2^9)^3/3!$.

It's true that every set of three *different* topping choices arises from 3! different length-3 sequences of choices. The mistake is that if some of the three choices are the same, then the set of three choices arises from *fewer* than 3! sequences. For example, if all three pizzas have the same toppings, there is only one sequence of topping choices for them.

One fix is to consider ways to choose toppings with 1,2 and 3 different topping choices. There are $2^9(2^9-1)(2^9-2)/3!$ ways to choose a set of 3 different choices, $2^9(2^9-1)$ ways to choose one topping choice to be used on two pizzas and a second choice for the third pizza, and 2^9 ways to choose one topping for all three pizzas, giving

$$\frac{2^9(2^9-1)(2^9-2)}{3!} + 2^9(2^9-1) + 2^9 = 22,500,864.$$

ways to choose three pizzas.

Alternatively, we can observe that this is exactly the problem of selecting a dozen donuts of five possible different kinds – except now there are 3 donuts and 2^9 kinds. Hence, there is a bijection

to the number of (2^9+2)-bit strings with exactly 2^9-1 ones and 3 zeros:

$$\binom{2^9+2}{3} = 22,500,864.$$

■

Problem 6. **(a)** In how many different ways can Blockbuster arrange 64 copies of *13 conversations about one thing*, 96 copies of *L'Auberge Espagnole* and 1 copy of *Matrix Revolutions* on a shelf? What if they are to be arranged in 5 shelves?

Solution. For 1 shelf, this is the number of ways to arrange 64 C's, 96 A's, and 1 M. By the bookeeper rule:

$$\frac{(64+96+1)!}{64!\ 96!\ 1!}$$

For 5 shelves, we can do the simple trick of introducing the dividers between the shelves as new objects. That is, we want the number of ways to arrange 64 C's, 96 A's, 1 M, and 4 X's (dividers). By the bookeeper theorem, again:

$$\frac{(64+96+1+4)!}{64!\ 96!\ 1!\ 4!}$$

■

(b) Set A has r elements and set B has n elements. How many functions are there from A to B? How many of them are injective (one-to-one)? How many of them are bijective?

Solution. Say $A = \{a_1, \ldots, a_r\}$ and $B = \{b_1, \ldots, b_n\}$ and consider the mapping that sends every function $f : A \to B$ to the sequence $(f(a_1), \ldots, f(a_r))$. This is a bijection between functions from A to B and r-long sequences of elements from B. By the product rule, the number of such sequences is

$$\underbrace{n \cdot n \cdots n}_{r \text{ times}} = n^r.$$

For injections, first note that (by the pigeonhole principle) there is no way to inject A into B if B has fewer elements than A. That is: if $r > n$, then the number of injections from A to B is 0. If $r \leq n$, though, the same mapping as previously becomes a bijection between injections from A to B and r-long sequences of *distinct* elements from B. By the generalized product rule, the number of such sequences is

$$n \cdot (n-1) \cdot (n-2) \cdots (n-r+1) = \frac{n!}{(n-r)!},$$

that is, the number of r-permutations of n elements.

For bijections, we similarly note that in the case $r \neq n$ the number of bijections from A to B is 0. If $r = n$, then a function from A to B is a bijection iff it is an injection. So the number

of bijections equals the number of injections: $n!/(n-n)! = n!$, which is exactly the number of different permutations of n elements.

Notice how *functions*, *injections*, and *bijections* correspond respectively to *sequences*, *r-permutations*, and *permutations*. ■

(c) Find the number of 5-card hands in which every suit appears at most twice.

Solution. There are two cases. Either one suit appears twice or else two suits appear twice. The number of hands in which one suit appears twice is $\binom{13}{2} \cdot 13^3 \cdot 4$, since there are 4 ways to choose the doubly-represented suit, $\binom{13}{2}$ ways to choose two values from this suit, and 13^3 ways to choose values for cards in the three remaining suits. Similarly, the number of hands in which two suits appear twice is $\binom{13}{2}^2 \cdot 13 \cdot \binom{4}{2} \cdot 2$. Therefore, there are a total of

$$\binom{13}{2} \cdot 13^3 \cdot 4 + \binom{13}{2}^2 \cdot 13 \cdot \binom{4}{2} \cdot 2$$

such hands. ■

(d) How many paths are there from point $(0,0)$ to $(50,50)$ if every step increments one coordinate and leaves the other unchanged? if there are impassable boulders sitting at points $(10,10)$ and $(20,20)$? *Hint:* Count the number of paths going through $(10,10)$, the number through $(20,20)$, and use Inclusion-Exclusion.

Solution. We use inclusion-exclusion. The total number of paths is $\binom{100}{50}$, but we must subtract off the obstructed paths. There are $\binom{20}{10} \cdot \binom{80}{40}$ paths through the first boulder, since there are $\binom{20}{10}$ paths from the start to the boulder and $\binom{80}{40}$ paths from the boulder to the finish. Similarly, there are $\binom{40}{20} \cdot \binom{60}{30}$ paths through the second boulder. However, we must subtract off paths going through both boulders, and there are $\binom{20}{10} \cdot \binom{20}{10} \cdot \binom{60}{30}$ of those. Therefore, the total number of paths is:

$$\binom{100}{50} - \binom{20}{10} \cdot \binom{80}{40} - \binom{40}{20} \cdot \binom{60}{30} + \binom{20}{10} \cdot \binom{20}{10} \cdot \binom{60}{30}$$

■

Solutions to In-Class Problems Week 11, Wed.

Problem 1. Define the function $f : \mathbb{N} \to \mathbb{N}$ recursively by the rules

$$\begin{aligned} f(0) &= 1, \\ f(1) &= 6, \\ f(n) &= 2f(n-1) + 3f(n-2) + 4 \qquad \text{for } n \geq 2. \end{aligned}$$

(a) Find a closed form for the generating function

$$G(x) ::= f(0) + f(1)x + f(2)x^2 + \cdots + f(n)x^n + \cdots .$$

Solution.

$$\begin{array}{rcccccccc} G(x) & = & f(0) & + & f(1)x & + & f(2)x^2 & +\cdots & + & f(n)x^n + \cdots \\ 2xG(x) & = & & & 2f(0)x & + & 2f(1)x^2 & +\cdots & + & 2f(n-1)x^n + \cdots \\ 3x^2G(x) & = & & & & & 3f(0)x^2 & +\cdots & + & 3f(n-2)x^n + \cdots \\ 4/(1-x) & = & 4 & + & 4x & & 4x^2 & +\cdots & + & 4x^n + \cdots \end{array}$$

Therefore,

$$\begin{aligned} G(x) &= 2xG(x) + 3x^2G(x) + \frac{4}{1-x} + (f(0) - 4) + (f(1) - 2f(0) - 4)x \\ &= 2xG(x) + 3x^2G(x) + \frac{4}{1-x} + (1-4) + (6-2-4)x \\ &= 2xG(x) + 3x^2G(x) + \frac{4}{1-x} - 3, \end{aligned}$$

It follows that

$$G(x)(1 - 2x - 3x^2) = \frac{4}{1-x} - 3,$$

and hence

$$\begin{aligned} G(x) &= \frac{\dfrac{4}{1-x} - 3}{(1+x)(1-3x)} \\ &= \frac{4}{(1-x)(1+x)(1-3x)} - \frac{3}{(1+x)(1-3x)} \\ &= \frac{4 - 3(1-x)}{(1-x)(1+x)(1-3x)} \\ &= \frac{3x+1}{(1-x)(1+x)(1-3x)}. \end{aligned} \tag{1}$$

■

(b) Find a closed form for $f(n)$. *Hint:* Find numbers a, b, c, d, e, g such that

$$G(x) = \frac{a}{1+dx} + \frac{b}{1+ex} + \frac{c}{1+gx}.$$

Solution. From (1) and the method of partial fractions, we conclude that $d, e, g = -1, 1, -3$, respectively. So we want a, b, c such that

$$\frac{3x+1}{(1-x)(1+x)(1-3x)} = \frac{a}{1-x} + \frac{b}{1+x} + \frac{c}{1-3x} \tag{2}$$

$$3x+1 = a(1+x)(1-3x) + b(1-x)(1-3x) + c(1-x)(1+x). \tag{3}$$

Setting $x = 1$ in (3), we conclude that $4 = a \cdot 2 \cdot (-2)$, so

$$a = -1.$$

Setting $x = -1$ in (3), we conclude that $4 - 3 \cdot 2 = b \cdot 2 \cdot 4$, so

$$b = -\frac{1}{4}.$$

Setting $x = 1/3$ in (3), we conclude that $4 - 3(2/3) = c \cdot (2/3)(4/3)$, so

$$c = \frac{9}{4}.$$

So from (1) and (2), we have

$$G(x) = \frac{-1}{1-x} + \frac{1/4}{1+x} + \frac{9/4}{1-3x}.$$

Now the coefficient of x^n in $a/(1-x)$ is a, the coefficient in $b/(1+x)$ is $b(-1)^n$ and the coefficient in $c/(1-3x)$ is $c3^n$. For $n \geq 2$, the coefficient in $G(x)$ is the sum of these coefficients. So

$$f(n) = -1 + \frac{(-1)^n}{4} + \frac{9}{4}3^n = \frac{3^{n+2} + (-1)^n}{4} - 1.$$

■

Appendix

Finding a Generating Function for Fibonacci Numbers

The Fibonacci numbers are defined by:

$$\begin{aligned} f_0 &::= 0 \\ f_1 &::= 1 \\ f_n &::= f_{n-1} + f_{n-2} \qquad (\text{for } n \geq 2) \end{aligned}$$

Let F be the generating function for the Fibonacci numbers, that is,

$$F(x) ::= f_0 + f_1 x + f_2 x^2 + f_3 x^3 + f_4 x^4 + \cdots$$

So we need to derive a generating function whose series has coefficients:

$$\langle 0,\ 1,\ f_1 + f_0,\ f_2 + f_1,\ f_3 + f_2,\ \ldots \rangle$$

Now we observe that

$$\begin{array}{rccccccccc}
 & \langle & 0, & 1, & 0, & 0, & 0, & \ldots & \rangle & \longleftrightarrow & x \\
 & \langle & 0, & f_0, & f_1, & f_2, & f_3, & \ldots & \rangle & \longleftrightarrow & xF(x) \\
+ & \langle & 0, & 0, & f_0, & f_1, & f_2, & \ldots & \rangle & \longleftrightarrow & x^2F(x) \\
\hline
 & \langle & 0, & 1+f_0, & f_1+f_0, & f_2+f_1, & f_3+f_2, & \ldots & \rangle & \longleftrightarrow & x + xF(x) + x^2F(x)
\end{array}$$

This sequence is almost identical to the right sides of the Fibonacci equations. The one blemish is that the second term is $1 + f_0$ instead of simply 1. But since $f_0 = 0$, the second term is ok.

So we have

$$\begin{aligned} F(x) &= x + xF(x) + x^2F(x). \\ F(x) &= \frac{x}{1 - x - x^2}. \end{aligned} \tag{4}$$

Finding a Closed Form for the Coefficients

Now we expand the righthand side of (4) into partial fractions. To do this, we first factor the denominator

$$1 - x - x^2 = (1 - \alpha_1 x)(1 - \alpha_2 x)$$

where $\alpha_1 = \frac{1}{2}(1 + \sqrt{5})$ and $\alpha_2 = \frac{1}{2}(1 - \sqrt{5})$ by the quadratic formula. Next, we find A_1 and A_2 which satisfy:

$$F(x) = \frac{x}{1 - x - x^2} = \frac{A_1}{1 - \alpha_1 x} + \frac{A_2}{1 - \alpha_2 x} \tag{5}$$

Now the coefficient of x^n in $F(x)$ will be A_1 times the coefficient of x^n in $1/(1 - \alpha_1 x)$ plus A_2 times the coefficient of x^n in $1/(1 - \alpha_2 x)$. The coefficients of these fractions will simply be the terms α_1^n and α_2^n because

$$\begin{aligned} \frac{1}{1 - \alpha_1 x} &= 1 + \alpha_1 x + \alpha_1^2 x^2 + \cdots \\ \frac{1}{1 - \alpha_2 x} &= 1 + \alpha_2 x + \alpha_2^2 x^2 + \cdots \end{aligned}$$

by the formula for geometric series.

So we just need to find find A_1 and A_2. We do this by plugging values of x into (5) to generate linear equations in A_1 and A_2. It helps to note that from (5), we have

$$x = A_1(1 - \alpha_2 x) + A_2(1 - \alpha_1 x),$$

so simple values to use are $x = 0$ and $x = 1/\alpha_2$. We can then find A_1 and A_2 by solving the linear equations. This gives:

$$A_1 = \frac{1}{\alpha_1 - \alpha_2} = \frac{1}{\sqrt{5}}$$
$$A_2 = -A_1 = -\frac{1}{\sqrt{5}}$$

Substituting into (5) gives the partial fractions expansion of $F(x)$:

$$F(x) = \frac{1}{\sqrt{5}}\left(\frac{1}{1-\alpha_1 x} - \frac{1}{1-\alpha_2 x}\right).$$

So we conclude that the coefficient, f_n, of x^n in the series for $F(x)$ is

$$\begin{aligned} f_n &= \frac{\alpha_1^n - \alpha_2^n}{\sqrt{5}} \\ &= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right) \end{aligned}$$

Solutions to In-Class Problems Week 12, Wed.

Problem 1. A Barglesnort makes its lair in one of three caves:

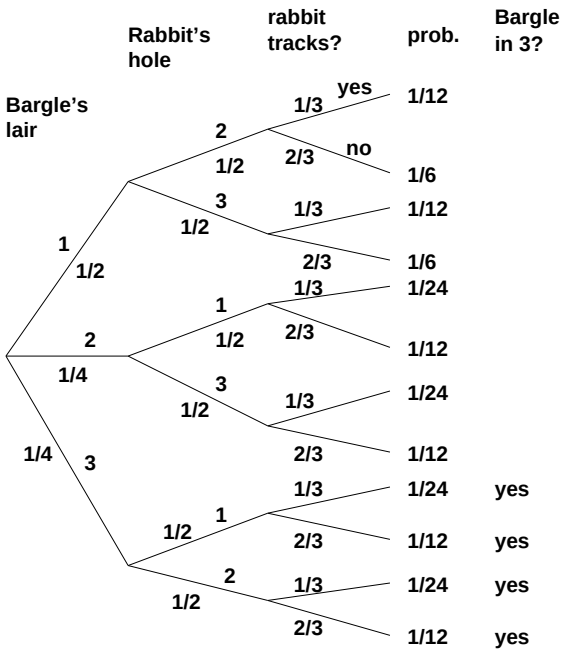
The Barglesnort inhabits cave 1 with probability $1/2$, cave 2 with probability $1/4$, and cave 3 with probability $1/4$. A rabbit subsequently moves into one of the two unoccupied caves, selected with equal probability. With probability $1/3$, the rabbit leaves tracks at the entrance to its cave. (Barglesnorts are much too clever to leave tracks.) What is the probability that the Barglesnort lives in cave 3, given that there are no tracks in front of cave 2?

Use a tree diagram and the four-step method.

Solution. A tree diagram is given below. Let B_3 be the event that the Barglesnort inhabits cave 3, and let T_2 be the event that there are tracks in front of cave 2. Taking data from the tree diagram, we can compute the desired probability as follows:

$$\begin{aligned}\Pr\left\{B_3 \mid \overline{T_2}\right\} &= \frac{\Pr\left\{B_3 \cap \overline{T_2}\right\}}{\Pr\left\{\overline{T_2}\right\}} \\ &= \frac{\frac{1}{24} + \frac{1}{12} + \frac{1}{12}}{1 - \frac{1}{12} - \frac{1}{24}} \\ &= \frac{5}{21}\end{aligned}$$

In the denominator, we apply the formula $\Pr\left\{\overline{T_2}\right\} = 1 - \Pr\{T_2\}$ for convenience.



■

Problem 2. There is a rare and deadly disease called *Nerditosis* which afflicts about 1 person in 1000. One symptom is a compulsion to refer to everything— fields of study, classes, buildings, etc.— using numbers. It's horrible. As victims enter their final, downward spiral, they're awarded a degree from MIT. Two doctors claim that they can diagnose Nerditosis.

(a) Doctor X received his degree from Harvard Medical School. He practices at Massachusetts General Hospital and has access to the latest scanners, lab tests, and research. Suppose you ask Doctor X whether you have the disease.

- If you have Nerditosis, he says "yes" with probability 0.99.
- If you don't have it, he says "no" with probability 0.97.

Let D be the event that you have the disease, and let E be the event that the diagnosis is erroneous. Use the Total Probability Law to compute $\Pr\{E\}$, the probability that Doctor X makes a mistake.

The Total Probability Law is

$$\Pr\{A\} = \Pr\{A \mid E\} \cdot \Pr\{E\} + \Pr\left\{A \mid \overline{E}\right\} \cdot \Pr\left\{\overline{E}\right\}.$$

Solution. By the Total Probability Law:

$$\begin{aligned}\Pr\{E\} &= \Pr\{E \mid D\} \cdot \Pr\{D\} + \Pr\left\{E \mid \overline{D}\right\} \cdot \Pr\left\{\overline{D}\right\} \\ &= 0.01 \cdot 0.001 + 0.03 \cdot 0.999 \\ &= 0.02998\end{aligned}$$

■

(b) "Doctor" Y received his genuine degree from a fully-accredited university for \$49.95 via a special internet offer. He knows that Nerditosis stikes 1 person in 1000, but is a little shakey on how to interpret this. So if you ask him whether you have the disease, he'll helpfully say "yes" with probability 1 in 1000 regardless of whether you actually do or not.

Let D be the event that you have the disease, and let F be the event that the diagnosis is faulty. Use the Total Probability Law to compute $\Pr\{F\}$, the probability that Doctor Y made a mistake.

Solution. By the Total Probability Law:

$$\begin{aligned}\Pr\{F\} &= \Pr\{F \mid D\} \cdot \Pr\{D\} + \Pr\left\{F \mid \overline{D}\right\} \cdot \Pr\left\{\overline{D}\right\} \\ &= 0.999 \cdot 0.001 + 0.001 \cdot 0.999 \\ &= 0.001998\end{aligned}$$

■

(c) Which doctor is more reliable?

Solution. Doctor X makes more than 15 times as many errors as Doctor Y. ■

Problem 3. Suppose there is a system with n components, and we know from past experience that any particular component will fail in a given year with probability p. That is, letting F_i be the event that the ith component fails within one year, we have

$$\Pr\{F_i\} = p$$

for $1 \leq i \leq n$. The *system* will fail if *any one* of its components fails. What can we say about the probability that the system will fail within one year?

Let F be the event that the system fails within one year. Without any additional assumptions, we can't get an exact answer for $\Pr\{F\}$. However, we can give useful upper and lower bounds, namely,

$$p \leq \Pr\{F\} \leq np. \tag{1}$$

So for example, if $n = 100$ and $p = 10^{-5}$, we conclude that there is at most one chance in 1000 of system failure within a year and at least one chance in 100,000.

Let's model this situation with the sample space $\mathcal{S} ::= \mathcal{P}(\{1, \ldots, n\})$ of subsets of positive integers $\leq n$, where $s \in \mathcal{S}$ corresponds to the indices of the components which fail within one year. For example, $\{2, 5\}$ is the outcome that the second and fifth components failed within a year and none of the other components failed. So the outcome that the system did not fail corresponds to the emptyset, $\emptyset$.

(a) Show that the probability that the system fails could be as small as p by describing appropriate probabilities for the sample points.

Solution. There could be a probability p of system failure if the all individual failures occur together. That is, let $\Pr\{\{1, \ldots, n\}\} ::= p$, $\Pr\{\emptyset\} ::= 1 - p$, and let the probability of all other outcomes be zero. So $F_i = \{s \in \mathcal{S} \mid i \in s\}$ and $\Pr\{F_i\} = 0 + 0 + \cdots + 0 + \Pr\{\{1, \ldots, n\}\} = \Pr\{\{1, \ldots, n\}\} = p$. Also, the only outcome with positive probability in F is $\{1, \ldots, n\}$, so $\Pr\{F\} = p$, as required. ■

(b) Show that the probability that the system fails could actually could be as large as np by describing appropriate probabilities for the sample points.

Solution. Suppose at most one component ever fails at a time. That is, $\Pr\{\{i\}\} = p$ for $1 \leq i \leq n$, $\Pr\{\emptyset\} = 1 - np$, and probability of all other points is zero. The sum of the probabilities of all the points is one, so this is a well-defined probability space. Also, the only sample point in F_i with positive probability is $\{i\}$, so $\Pr\{F_i\} = \Pr\{\{i\}\} = p$ as required. Finally, $\Pr\{F\} = np$ because $F = \{A \subseteq \{1, \ldots, n\} \mid A \neq \emptyset\}$, so F in particular contains all the n outcomes of the form $\{i\}$. ■

(c) Prove the inequality (1).

Solution. $F = \bigcup_{i=1}^{n} F_i$ so

$$\begin{aligned}
p &= \Pr\{F_1\} && \text{(given)} && (2)\\
&\leq \Pr\{F\} = \Pr\left\{\bigcup F_i\right\} && \text{(def. of } F\text{)} && (3)\\
&\leq \sum_{i=1}^{n} \Pr\{F_i\} && \text{(Union bound)} && (4)\\
&= np. && && (5)
\end{aligned}$$

■

Problem 4. There were n Immortal Warriors born into our world, but in the end *there can be only one*. The Immortals' original plan was to stalk the world for centuries, dueling one another with ancient swords in dramatic landscapes until only one survivor remained. However, after a thought-provoking discussion of probabilistic independence, they opt to give the following protocol a try:

1. The Immortals forge a coin that comes up heads with probability p.
2. Each Immortal flips the coin once.
3. If *exactly one* Immortal flips heads, then he or she is declared The One. Otherwise, the protocol is declared a failure, and they all go back to hacking each other up with swords.

(a) One of the Immortals (Kurgan from the Russian steppe) argues that as n grows large, the probability that this protocol succeeds must tend to zero. Another (McLeod from the Scottish highlands) argues that this need not be the case, provided p is chosen *very carefully*. What does your intuition tell you?

Solution. Your intuition tells you that a short nap would be nice right now. As would a couple cookies to dunk in a cold glass of milk. ■

(b) What is the probability that the experiment succeeds as a function of p and n?

Solution. The sample space consists of all possible results of n coin flips, which we can represent by the set $\{H, T\}^n$. Let E be the event that the experiment successfully selects The One. Then E consists of the n outcomes which contain a single head. In general, the probability of an outcome with h heads and $n - h$ tails is:

$$p^h(1-p)^{n-h}$$

Summing the probabilities of the n outcomes in E gives the probability that the procedure succeeds:

$$\Pr\{E\} \quad = \quad np(1-p)^{n-1}$$

■

(c) How should p, the bias of the coin, be chosen in order to maximize the probability that the experiment succeeds? (You're going to have to compute a derivative!)

Solution. We compute the derivative of the success probability:

$$\frac{d}{dp}\, np(1-p)^{n-1} \;=\; n(1-p)^{n-1} - np(n-1)(1-p)^{n-2}$$

Now we set the right side equal to zero to find the best probability p:

$$\begin{aligned} n(1-p)^{n-1} &= np(n-1)(1-p)^{n-2} \\ (1-p) &= p(n-1) \\ p &= 1/n \end{aligned}$$

This answer makes sense, since we want the coin to come up heads exactly 1 time in n. ■

(d) What is the probability of success if p is chosen in this way? What quantity does this approach when n, the number of Immortal Warriors, grows large?

Solution. Setting $p = 1/n$ in the formula for the probability that the experiment succeeds gives:

$$\Pr\{E\} \;=\; \left(1 - \frac{1}{n}\right)^{n-1}$$

In the limit, this tends to $1/e$. McLeod is right. ■

Solutions to In-Class Problems Week 13, Wed.

Problem 1. The following two parts are not related. Try them, to make sure you understand the jargon of random variables, distributions, probability density functions, etc. Ask your TA if you don't understand/remember what some phrase means.

(a) Suppose X_1, X_2, and X_3 are three mutually independent random variables, each having the uniform distribution

$$\Pr\{X_i = k\} \text{ equal to } 1/3 \text{ for each of } k = 1, 2, 3.$$

Let M be another random variable giving the maximum of these three random variables. What is the density function of M?

Solution. This can be hashed out by counting the possible outcomes. Alternatively, we can reason as follows:

The event $M = 1$ is the event that all three of the variables equal 1, and since they are mutually independent, we have

$$\Pr\{M = 1\} = \Pr\{X_1 = 1\} \cdot \Pr\{X_2 = 1\} \cdot \Pr\{X_3 = 1\} = \left(\frac{1}{3}\right)^3 = \frac{1}{27}.$$

To compute $\Pr\{M = 2\}$, we first compute $\Pr\{M \leq 2\}$. Now the event $[M \leq 2]$ is the event that all three of the variables is at most 2, so by mutual independence we have

$$\Pr\{M \leq 2\} = \Pr\{X_1 \leq 2\} \cdot \Pr\{X_2 \leq 2\} \cdot \Pr\{X_3 \leq 2\} = \left(\frac{2}{3}\right)^3 = \frac{8}{27}.$$

Therefore,

$$\Pr\{M = 2\} = \Pr\{M \leq 2\} - \Pr\{M = 1\} = \frac{8}{27} - \frac{1}{27} = \frac{7}{27}.$$

Finally,

$$\Pr\{M = 3\} = 1 - \Pr\{M \leq 2\} = 1 - \frac{8}{27} = \frac{19}{27}.$$

■

(b) Suppose X, Y are two independent binomial random variables with parameters (n, p) and (m, p), respectively. What is $\Pr\{X + Y = k\}$?

Solution. The PDF of X is the probability of tossing k Heads out of n independent flips of a coin with bias p. Likewise for Y and m flips. Since, X and Y are independent, the PDF of $X + Y$ corresponds to $n+m$ independent flips, i.e., $X+Y$ is a Binomial variable with parameters $(n+m, p)$. Hence,

$$\binom{m+n}{k} p^k (1-p)^{m+n-k}.$$

■

Problem 2. I know everything. Seriously. So, I know everything that everybody thinks. In particular, I know who each one of the 750 billion members of the galaxy want to vote for in the upcoming elections for the Intergalactic president. I know that a fraction $p = 0.52$ of them want to vote for the current president.

You are mortal. An insignificant dot in space-time. But a quite significant dot among dots. You work closely to the current Intergalactic president and, within a week, you must answer his agonizing question: "Am I winning?" Or, in math jargon (but with the same agony): "Is $p > 1/2$?"

Your *first* idea is to ask me (I know everything). But you haven't talked to me for a long time, so you know I won't tell you. Your *second* idea is to call every person in the galaxy, ask them, then divide the yes's by 750 billion. But you soon realize there is not enough time (there is a reason for representative democracy). Your *third* idea... You have no third idea! In your panic as the week is almost over, you start picking galaxy members at random, call them, and ask!

Amazingly, that's the correct approach. But you should be careful what you are going to say to the president! Let's see.

(a) In your first phone call, you pick one galaxy member *uniformly at random*, call, and ask whether he/she will vote for the president. What is the probability that the answer is going to be "yes"... (i) from my perspective? (ii) from your perspective? How would you model this in terms of coin flips?

Solution. From my perspective, it's 0.52. From your perspective, it is also 0.52. The only problem is that you don't know that, so you just call it p. Clearly, from your perspective, the first phone call is the same as flipping a coin with an *unknown* bias, which you call p (and I know is 0.52). ■

(b) In your second phone call, you again pick a galaxy member *uniformly at random*, call, and ask whether he/she will vote for the president. But wait! When selecting the second voter, shouldn't you exclude the guy that you asked in the first phone call? Maybe, but what complication comes from excluding him/her?

Solution. If you do this, you alter the coin that you are flipping. The bias will decrease or increase, depending on whether the first guy said "yes" or "no", respectively. The analysis gets messy, so you don't want to do this. ■

(c) So, in each one of n phone calls, you pick a galaxy member *uniformly at random* and ask. Your plan is to eventually divide the number, Y, of "yes" answers by n to get $P ::= Y/n$. An MIT friend tells you that, as the numerical outcome of a random experiment, this P is a random variable, and that, according to his calculations,

$$\Pr\{|P - p| \leq 0.03\} \quad \geq \quad 0.95.$$

When you are done calling people, you divide to get P, and it's 0.53. You call the president up and... what do you say?

(1) Mr. President, $p = 0.53$!

(2) Mr. President, with probability at least 95%, p is within 0.03 of 0.53!

(3) Mr. President, either p is within 0.03 of 0.53 or something very strange (less than 5-in-100) has happened.

For each statement answer: (i) Are you justified to claim it? (ii) Is it true?

Solution. Statement (1) is clearly off the mark.

(i) Since you haven't asked all galaxy members, you can only make probabilistic statements about p.

(ii) Statement (1) is also false, since $p = 0.52$. However, with a different choice of voters, it could have been true. Of course, even in that case, you wouldn't be justified in making it.

It would be wrong for you to make statement (2).

(i) The unknown fraction, p, is a *constant*, not a random variable. It is *either* within 0.03 of 0.53, *or* more than 0.03 away of 0.53. It doesn't make much sense to talk about the probability that it has this, or any other, property: it does or it doesn't. And since you don't know which case holds, it would be wrong for you to make statement (2) about p.

(ii) Now you could argue that statement (2) is actually true in this case. Namely, since the constant p is 0.52, it is indeed within 0.03 of 0.53. So you might claim that the probability in question is actually 1, and therefore is indeed at least 95%. But introducing probability in this way is misleading, at best.

Statement (3) is the correct one.

(i) You are justified in making statement (3). To see why, start with the statement

$$\textit{either} \quad |0.53 - p| \leq 0.03 \qquad \textit{or} \quad |0.53 - p| > 0.03.$$

which is clearly true. Now read it as follows: *Either* p is within 0.03 of 0.53 *or* it is not and therefore my random random variable, P, took a value from a set that is hit only 5 times in 100. So, clearly *either* p is within 0.03 of 0.53, *or* something strange has happened.

(ii) Statement (3) is true. In this particular case, it is true because the first half of it is true. But it would still be true even if p was not within 0.03 of 0.53. That's because statement (3) is an assertion about the behavior of the random variable, P, that is true no matter what the value of p is, so you can legitimately make the statement without knowing what p really is.

■

A third problem that originally appeared here has been deleted. Few, if any, teams got to this problem; it will be postponed for a later class problem session.

Solutions to In-Class Problems Week 14, Wed.

Problem 1. Suppose you have learned that the average graduating MIT student's total number of credits is 200.

(a) Knowing only this average, use Markov's inequality to find a best possible upper bound for the fraction of MIT students graduating with at least 235 credits. [1]

Solution. Let X be a random variable with a distribution equal to that of the graduating MIT students' credit count. We are given that $\mathrm{E}[X] = 200$. By Markov's inequality:

$$\Pr\{X \geq 235\} \leq \frac{\mathrm{E}[X]}{235} = \frac{200}{235} \approx 0.85$$

■

(b) Demonstrate that this is a best possible bound by giving a distribution for which this bound holds with equality.

Solution. The bound is attained with equality at the two-point distribution which has non-zero values only at 0 and 235, that is,

$$\begin{aligned} \Pr\{X = 235\} &= \frac{200}{235} \\ \Pr\{X = 0\} &= \frac{35}{235} \\ \Pr\{X = x\} &= 0 \text{ for all other } x. \end{aligned}$$

■

(c) Suppose you are now told that no student can graduate with fewer than 170 units. How does this allow you to improve your previous bound? As before, show that this is the best possible bound.

[1] Ignore the fact that there are practical limits to the amount of time a student can stay at MIT and remain sane; That is, assume that there is no bound on the number of credits a student may earn.

Solution. We can now apply Markov's inequality to the nonnegative variable $Y = X - 170$, with expectation $\mathrm{E}[Y] = \mathrm{E}[X - 170] = \mathrm{E}[X] - 170 = 30$. So,

$$\Pr\{X \geq 235\} = \Pr\{X - 170 \geq 235 - 170\} = \Pr\{Y \geq 65\}$$

Therefore:

$$\begin{aligned} \Pr\{X \geq 235\} &= \Pr\{Y \geq 65\} \\ &\leq \frac{\mathrm{E}[Y]}{65} \\ &\leq \frac{30}{65} \approx 0.46 \end{aligned}$$

As above, we achieve an optimum (equality in the bound) when our distribution consists of two spikes: one at $(x - 170) = c - 170$, that is, $x = 235$, and one at $(x - 170) = 0$, that is, $x = 170$.

$$\begin{aligned} \Pr\{X = 235\} &= (200 - 170)/(235 - 170) = 30/65 \\ \Pr\{X = 170\} &= 35/65 \\ \Pr\{X = x\} &= 0 \text{ for all other } x \end{aligned}$$

■

(d) Now suppose you *further* learn that the standard deviation of the total credits per graduating student is 7. What is the Chebyshev bound on the fraction of students who can graduate with at least 235 credits?

Solution. The variance of X is the square of the standard deviation, or 49. The variance of Y is the same as that of X, by the linearity of variance. That is, $\mathrm{Var}[Y] = \mathrm{Var}[X - 170] = \mathrm{Var}[X] - \mathrm{Var}[170] = 49 - 0$. (The variance of a constant is 0).

$$\begin{aligned} \Pr\{X \geq 235\} &= \Pr\{Y \geq 65\} \\ &= \Pr\{Y - \mathrm{E}[Y] \geq 65 - \mathrm{E}[Y]\} \\ &= \Pr\{Y - 30 \geq 35\} \\ &\leq \Pr\{|Y - 30| \geq 35\} \\ &\leq \frac{\mathrm{Var}[Y]}{35^2} \\ &\leq \frac{49}{1225} = \frac{1}{25} \end{aligned}$$

This is a much better bound than before! ■

Problem 2. **(a)** Show that Markov's Theorem only applies to nonnegative random variables. That is, give an example of a random variable to which Markov's Theorem gives a *wrong* answer.

Solution. Here is one possible answer: Let R be -10 with probability $1/2$ and 10 with probability $1/2$. Then we have:

$$\mathrm{E}[R] = -10 \cdot \frac{1}{2} + 10 \cdot \frac{1}{2} = 0$$

Suppose that we now tried to compute $\Pr\{R \geq 5\}$ using Markov's Theorem:

$$\Pr\{R \geq 5\} \leq \frac{\mathrm{E}[R]}{5} = \frac{0}{5} = 0.$$

This is the wrong answer! Obviously, R is at least 5 with probability $1/2$. ■

(b) Suppose R is a random variable that is always at least -10 and has expectation 0. Since R may be negative, Markov's theorem does not apply directly. Still, use Markov's theorem to show that the probability that R is ≥ 5 is at most $2/3$.

Solution. Let $T ::= R + 10$. Now T is a nonnegative random variable with expectation $\mathrm{E}[R + 10] = \mathrm{E}[R] + 10 = 10$, so Markov's Theorem applies and tells us that $\Pr\{T \geq 15\} \leq 10/15 = 2/3$. But $T \geq 15$ iff $R \geq 5$, so $\Pr\{R \geq 5\} \leq 2/3$. ■

Problem 3. There are n people at a circular table in a Chinese restaurant. On the table, there are n different appetizers arranged on a big Lazy Susan. Each person starts munching on the appetizer directly in front of him or her. Then someone spins the Lazy Susan so that everyone is faced with a random appetizer. In class, we saw that the expected number of people that end up with the appetizer that they had originally is 1.

Let X_i be the indicator variable for the ith person getting their own appetizer back. Let S_n be the total number of people who get their own appetizer back, so $S_n = \sum_{i=1}^{n} X_i$.

(a) What is $\mathrm{E}[X_i^2]$?

Solution. $X_i = 1$ with probability $1/n$ and 0 otherwise. Thus $X_i^2 = 1$ with probability $1/n$ and 0 otherwise. So $\mathrm{E}[X_i^2] = 1/n$. ■

(b) For $i \neq j$, what is $\mathrm{E}[X_i X_j]$?

Solution. The probability that X_i and X_j are both 1 is $1/n$. Thus $X_i X_j = 1$ with probability $1/n$, and is zero otherwise. So $\mathrm{E}[X_i X_j] = 1/n$. ■

(c) What is $\mathrm{E}[S_n^2]$?

Solution.

$$\begin{aligned}\mathrm{E}\left[S_n^2\right] &= \sum_{i,j} \mathrm{E}[X_i X_j] \\ &= n^2 \cdot \frac{1}{n} \\ &= n.\end{aligned}$$

Alternatively, we observe directly that

$$\Pr\left\{S_n^2 = n^2\right\} \Pr\{S_n = n\} = \frac{1}{n}$$

and

$$\Pr\left\{S_n^2 = 0\right\} \Pr\{S_n = 0\} = \frac{n-1}{n},$$

so

$$\mathrm{E}\left[S_n^2\right] = n^2 \frac{1}{n} + 0 \cdot \frac{n-1}{n} = n.$$

■

(d) What is $\mathrm{Var}[S_n]$?

Solution.

$$\begin{aligned}\mathrm{Var}[S_n] &= \mathrm{E}\left[S_n^2\right] - \mathrm{E}^2[S_n] \\ &= n - 1^2 \\ &= n - 1.\end{aligned}$$

■

(e) Discuss the accuracy of the Chebyshev Bound on the probability that S_n is distance x from its expectation as x ranges over integers between 1 and n.

Solution. The bound $\mathrm{Var}[S_n]/x^2$ is trivial (> 1) unless $x^2 > varianceS_n$, that is, unless $x \geq \left\lfloor \sqrt{n-1} + 1 \right\rfloor$. In the case that x equals this minimum value, it still gives yields a near trivial bound of $(n-1)/\left\lfloor \sqrt{n-1} + 1 \right\rfloor \approx 1$, whereas actually,

$$\Pr\{|S_n - 1| \geq x\} = \frac{1}{n}$$

for all $x \leq n-1$, and

$$\Pr\{|S_n - 1| \geq x\} = 0$$

for $x > n-1$. At $x = n-1$, the Chebyshev Bound is $(n-1)/(n-1)^2 = 1/(n-1)$ which is still a bit larger than the actual value of $1/n$. Finally, at $x = n$, the Chebyshev Bound is $(n-1)/n^2 = 1/n - 1/n^2$ whereas the actual probability is zero. ■

Problem 4. For any random variable, R, with $\mathrm{E}[R] = \mu$ and $\mathrm{Var}[R] = v$, the Chebyshev Bound says that for any real number $x > 0$,

$$\Pr\{|R - \mu| \geq x\} \leq \frac{v}{x^2}.$$

Show that for any real number, μ, and real numbers $v, x > 0$, there is an R for which the Chebyshev Bound is tight, that is,

$$\Pr\{|R| \geq x\} = \frac{v}{x^2}. \tag{1}$$

Hint: Assume $\mu = 0$ and let R be three valued with values $0, -x$, and x.

Solution. From the hint, we aim to find an R with $\mathrm{E}[R] = 0$ and $\mathrm{Var}[R] = v$ that satisfies equation (1).

Using the further hint that R takes only values $0, -x, x$, we have

$$0 = \mathrm{E}[R] = x\Pr\{R = x\} - x\Pr\{R = -x\} = x\left(\Pr\{R = x\} - \Pr\{R = -x\}\right)$$

so

$$\Pr\{R = x\} = \Pr\{R = -x\}, \tag{2}$$

since $x > 0$. Also,

$$v = \mathrm{Var}[R] = \mathrm{E}\left[R^2\right] = x^2\Pr\{R = -x\} + x^2\Pr\{R = x\} = 2x^2\Pr\{R = x\},$$

so

$$\Pr\{R = x\} = \frac{v}{2x^2}.$$

This implies

$$\Pr\{R = 0\} = 1 - \Pr\{R = -x\} - \Pr\{R = x\} = 1 - \frac{v}{x^2},$$

which completely determines the distribution of R. Moreover,

$$\Pr\{|R| \geq x\} = \Pr\{R = -x\} + \Pr\{R = x\} = \frac{v}{x^2}$$

which confirms (1).

Finally, given μ, x, and v, if we let $R' ::= R + \mu$, then R' will be the desired random variable for which the Chebyshev Bound is tight. ■

Problem 5. The covariance, $\text{Cov}[X, Y]$, of two random variables, X and Y, is defined to be $\text{E}[XY] - \text{E}[X]\,\text{E}[Y]$. Note that if two random variables are independent, then their covariance is zero.

(a) Give an example to show that having $\text{Cov}[X, Y] = 0$ does not necessarily mean that X and Y are independent.

Solution. Let (X, Y) have joint probability given by the table below:

X	Y	P
-1	1	$1/3$
0	0	$1/3$
1	1	$1/3$

Note that X and Y are not independent:

$$\Pr\{X = 1 \;\&\; Y = 1\} = 1/3 \neq 2/9 = \Pr\{X = 1\}\Pr\{Y = 1\}.$$

But since $XY = X$ and $\text{E}[X] = 0$, we have

$$\text{E}[X]\,\text{E}[Y] = 0 \cdot \text{E}[Y] = 0 = \text{E}[X] = \text{E}[XY].$$

Thus $\text{Cov}[X, Y] = 0$. ■

(b) Let $X_1, \ldots, X_n$ be random variables. Prove that

$$\text{Var}[X_1 + \cdots + X_n] = \sum_{i=1}^{n} \text{Var}[X_i] + 2\sum_{i<j} \text{Cov}[X_i, X_j].$$

Solution.

$$\begin{aligned}
\text{Var}[X_1 + \cdots + X_n] &= \text{E}\left[(X_1 + \cdots + X_n)^2\right] - \text{E}^2[X_1 + \cdots + X_n] \\
&= \text{E}\left[\sum_i X_i^2 + (\sum_{i<j} 2X_iX_j)\right] - \left(\sum_i \text{E}[X_i]^2 + \sum_{i<j} 2\,\text{E}[X_i]\,\text{E}[X_j]\right) \\
&= \sum_i \text{E}\left[X_i^2\right] + \sum_{i<j} 2\,\text{E}[X_iX_j] - \sum_i \text{E}[X_i]^2 - \sum_{i<j} 2\,\text{E}[X_i]\,\text{E}[X_j] \\
&= \sum_i \text{E}\left[X_i^2\right] - \text{E}[X_i]^2 + \sum_{i<j} 2(\text{E}[X_iX_j] - \text{E}[X_i]\,\text{E}[X_j]) \\
&= \sum_i \text{Var}[X_i] + 2\sum_{i<j} \text{Cov}[X_i, X_j].
\end{aligned}$$

■

Solutions to In-Class Problems Week 15, Wed.

Gamblers Ruin

A gambler aims to gamble until he reaches a *goal* of T dollars or until he runs out of money, in which case he is said to be "ruined." He gambles by making a sequence of 1 dollar bets. If he wins an individual bet, his stake increases by one dollar. If he loses, his stake decreases by one dollar. In each bet, he wins with probability $p > 0$ and loses with probability $q ::= 1 - p > 0$. He is an overall *winner* if he reaches his goal and is an overall *loser* if he gets ruined.

In a *fair* game, $p = q = 1/2$. The gambler is more likely to win if $p > 1/2$ and less likely to win if $p < 1/2$.

With T and p fixed, the gambler's probability of winning will depend on how much money he starts with. Let w_n be the probability that he is a winner when his initial stake in n dollars.

Problem 1. **(a)** What are w_0 and w_T?

Solution. $w_0 = 0$ and $w_T = 1$. ■

(b) Note that w_n satisfies a linear recurrence

$$w_{n+1} = aw_n + bw_{n-1} \tag{1}$$

for some constants a, b and $0 < n < T$. Write simple expressions for a and b in terms of p.

Solution. By Total Probability

$$\begin{aligned} w_n &= \Pr\{\text{win game} \mid \text{win the first bet}\}\Pr\{\text{win the first bet}\} + \\ &\quad \Pr\{\text{win game} \mid \text{lose the first bet}\}\Pr\{\text{lose the first bet}\} \\ &= pw_{n+1} + q\Pr\{w_{n-1}\}, \qquad \text{so} \\ pw_{n+1} &= w_n - qw_{n-1} \\ w_{n+1} &= \frac{w_n}{p} - \frac{qw_{n-1}}{p}. \end{aligned} \tag{2}$$

(3)

So

$$a = \frac{1}{p}, \qquad b = -\frac{q}{p}.$$

■

(c) For $n > T$, let w_n be defined by the recurrence (1), and let $g(x) ::= \sum_{n=1}^{\infty} w_n x^n$ be the generating function for the sequence $w_0, w_1, \ldots$. Verify that

$$g(x) = \frac{w_1 x}{(1-x)(1-\frac{q}{p}x)}. \tag{4}$$

Solution.

$$\begin{array}{rcccccccc} g(x) & = & w_0 & + & w_1 x & + & w_2 x^2 & + & w_3 x^3 & +\cdots \\ xg(x)/p & = & & & w_0 x/p & + & w_1 x^2/p & + & w_2 x^3/p & +\cdots \\ (q/p)x^2 g(x) & = & & & & & (q/p)w_0 x^2 & + & (q/p)w_1 x^3 & +\cdots \end{array}$$

so

$$g(x) - \left(\frac{xg(x)}{p} - \frac{qx^2 g(x)}{p}\right) = w_0 + w_1 x - w_0 x/p = w_1 x,$$

$$g(x)\left(1 - \frac{x}{p} + \frac{qx^2}{p}\right) = w_1 x. \tag{5}$$

But

$$1 - \frac{x}{p} + \frac{qx^2}{p} = (1-x)(1-\frac{q}{p}x) \tag{6}$$

Combining (6) and (5) yields (4). ■

(d) Conclude that in an unfair game

$$w_n = c + d\left(\frac{q}{p}\right)^n \tag{7}$$

for some constants c, d.

Solution. In an unfair game $p/q \neq 1$, so from (4), we know that there will be c, d such that

$$g(x) = \frac{c}{1-x} + \frac{d}{1-\frac{q}{p}x} \tag{8}$$

so w_n will be the corresponding combination of the coefficients of x^n in $1/(1-x)$ and $1/(1-(q/p)x)$, namely, (7). ■

(e) Show that in an unfair game,

$$w_n = \frac{(q/p)^n - 1}{(q/p)^T - 1}.$$

Solution. Given (4), we want c, d such that

$$\frac{w_1 x}{(1-x)(1-\frac{q}{p}x)} = \frac{c}{1-x} + \frac{d}{1-\frac{q}{p}x}.$$

So c, d satisfy

$$w_1 x = c(1-\frac{q}{p}x) + d(1-x).$$

Letting $x = 1$ gives

$$c = \frac{w_1}{1-q/p}.$$

Letting $x = p/q$ gives

$$d = \frac{pw_1/q}{1-p/q} = \frac{w_1}{q/p-1} = -c.$$

So plugging into (7) gives

$$w_n = \frac{w_1}{q/p-1}\left(\left(\frac{q}{p}\right)^n - 1\right). \tag{9}$$

Now we can solve for w_1, by letting $n = T$ in (9):

$$1 = w_T = \frac{w_1}{q/p-1}\left(\left(\frac{q}{p}\right)^T - 1\right)$$

so

$$w_1 = \frac{(q/p-1)}{(q/p)^T - 1}.$$

Combining this with (9) yields

$$w_n = \frac{((q/p)^n - 1)}{(q/p)^T - 1}.$$

■

(f) Verify that if $0 < a < b$, then

$$\frac{a}{b} < \frac{a+1}{b+1}.$$

Conclude that if $p < 1/2$, then

$$w_n < \left(\frac{p}{q}\right)^{T-n}.$$

Solution.

$$\frac{a}{b} = \frac{a(1+1/b)}{b(1+1/b)} = \frac{a+a/b}{b+1} < \frac{a+1}{b+1}.$$

So from the previous part, we have

$$w_n = \frac{(q/p)^n - 1}{(q/p)^T - 1} < \frac{(q/p)^n}{(q/p)^T} = \left(\frac{q}{p}\right)^{n-T} = \left(\frac{p}{q}\right)^{T-n}.$$

■

Problem 2. Show that in a fair game,

$$w_n = \frac{w}{T}.$$

Hint: Use equation (4) again.

Solution. This time $p = q = 1/2$ so from (4),

$$g(x) = \frac{w_1 x}{(1-x)^2}.$$

Now we need a, b such that

$$\frac{w_1 x}{(1-x)^2} = \frac{a}{1-x} + \frac{b}{(1-x)^2}, \tag{10}$$

so we will have

$$w_n = a + b(n+1).$$

Solving for a, b, we have from (10)

$$w_1 x = a(1-x) + b.$$

Letting $x = 0$ yields $a = -b$ and $x = 1$ yields $b = w_1$, so

$$w_n = -w_1 + w_1(n+1) = w_1 n.$$

Also,

$$1 = w_T = w_1 T$$

so

$$w_1 = \frac{1}{T}$$

and hence

$$w_n = \frac{n}{T}.$$

■

Problem 3. Now suppose $T = \infty$, that is, the gambler keeps playing until he is ruined. (Now there may be a positive probability that he actually plays forever.) Let r be the probability that starting with $n > 0$ dollars, the gambler's stake ever gets reduced to $n - 1$.

(a) Explain why

$$r = q + pr^2.$$

Solution. By Total Probability

$$\begin{aligned} r &= \Pr\{\text{ever down \$1} \mid \text{lose the first bet}\} \Pr\{\text{lose the first bet}\} + \\ &\quad \Pr\{\text{ever down \$1} \mid \text{win the first bet}\} \Pr\{\text{win the first bet}\} \\ &= q + p \Pr\{\text{ever down \$1} \mid \text{win the first bet}\} \end{aligned}$$

But

$$\begin{aligned} &\Pr\{\text{ever down \$1} \mid \text{win the first bet}\} \\ &= \Pr\{\text{ever down \$2}\} \\ &= \Pr\{\text{being down the first \$1}\} \Pr\{\text{being down another \$1}\} \\ &= r^2. \end{aligned}$$

■

(b) Conclude that if $p \leq 1/2$, then $r = 1$.

Solution. $pr^2 - r + q$ has roots q/p and 1. So $r = 1$ or $r = q/p$. But $1 \leq r$, which implies $r = 1$ when $q/p \geq 1$, that is, when $p \leq 1/2$.

In fact $r = q/p$ when $q/p < 1$, namely, when $p > 1/2$, but this requires an additional argument that we omit. ■

(c) Conclude that even in a fair game, the gambler is sure to get ruined *no matter how much money he starts with*!

Solution. The gambler gets ruined starting with initial stake $n = 1$ precisely if his initial stake goes down by 1 dollar, so his probability of ruin is r, which equals 1 in the fair case.

The recurrence (1) will also hold in this $T = \infty$ case if we interpret w_n as the probability of *not* being ruined, that is, the gambler wins if he can gamble forever. So w_1 is the probability he is *not* getting ruined starting with a 1 dollar stake, that is $w_1 = 1 - r = 0$. Since $w_0 = 0 = w_1$, the recurrence implies that $w_n = 0$ for all $n \geq 0$. ■

(d) Let t be the expected time for the gambler's stake to go down by 1 dollar. Verify that

$$t = q + p(1 + 2t).$$

Conclude that starting with a 1 dollar stake in a fair game, the gambler can expect to play forever!

Solution. By Total Expectation

$$\begin{aligned} t &= \mathrm{E}\left[\#\text{steps to be down \$1} \mid \text{lose the first bet}\right] \Pr\{\text{lose the first bet}\} + \\ &\qquad \mathrm{E}\left[\#\text{steps to be down \$1} \mid \text{win the first bet}\right] \Pr\{\text{win the first bet}\} \\ &= q + p\,\mathrm{E}\left[1 + \#\text{steps to be down \$1} \mid \text{win the first bet}\right]. \end{aligned}$$

But

$$\begin{aligned} &\mathrm{E}\left[\#\text{steps to be down \$1} \mid \text{win the first bet}\right] \\ &= \mathrm{E}\left[\#\text{steps to be down \$2}\right] \\ &= \mathrm{E}\left[\#\text{steps to be down the first \$1}\right] + \mathrm{E}\left[\#\text{steps to be down another \$1}\right] \\ &= 2t. \end{aligned}$$

This implies the required formula $t = q + p(1 + 2t)$. If $p = 1/2$ we conclude that $t = 1 + t$, which means t must be infinite. ■

Solutions to In-Class Problems Week 1, Wed.

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

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

Bogus proof.

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

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

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

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

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

■

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

Bogus proof.

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

■

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

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

Problem 2.
It's a fact that the Arithmetic Mean is at least as large the Geometric Mean, namely,

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

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

Bogus proof.

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

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

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

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

Proof.

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

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

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

Bogus Claim: $0 = 1$.

Bogus proof.

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

which proves $0 = 1$. ■

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

Bogus proof.

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

So watch out for backward proofs!

■

Problem 3.
Albert announces that he plans a surprise 6.042 quiz next week. His students wonder if the quiz could be next Friday. The students realize that it obviously cannot, because if it hadn't been given before Friday, everyone would know that there was only Friday left on which to give it, so it wouldn't be a surprise any more.

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

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

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

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

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

6.042J / 18.062J Mathematics for Computer Science
Spring 2010

Solutions to In-Class Problems Week 1, Fri.

Problem 1.
Generalize the proof from lecture (reproduced below) that $\sqrt{2}$ is irrational, for example, how about $\sqrt[3]{2}$? Remember that an irrational number is a number that cannot be expressed as a ratio of two integers.

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

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

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

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

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

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

Since the assumption that $\sqrt{2}$ is rational leads to this contradiction, the assumption must be false. That is, $\sqrt{2}$ is indeed irrational. This italicized comment on the implication of the contradiction normally goes without saying, but since this is the first 6.042 exercise about proof by contradiction, we've said it.

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

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

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

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

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

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

$$d^2 = 2k^2. \tag{4}$$

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

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

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

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

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

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

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

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

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

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

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

There is a simple proof by contradiction: suppose to the contrary that a is odd. It's a familiar (and easily verified[1]) fact that the product of two odd numbers is odd, from which it follows that the product of *any* finite number of odd numbers is odd, so a^n would also be odd, contradicting the fact that a^n is even.

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

Problem 2.
Here is a generalization of Problem 1 that you may not have thought of:

Lemma 2.1. *Let the coefficients of the polynomial $a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} + x^m$ be integers. Then any real root of the polynomial is either integral or irrational.*

(a) Explain why Lemma (2.1) immediately implies that $\sqrt[m]{k}$ is irrational whenever k is not an mth power of some integer.

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

Solution. Saying that an integer, k, is not the nth power of an integer, is equivalent to saying that the equation $x^M = k$ has no integer solutions. Another way to say this is that the polynomial $x^m - k$ has no integer root. Lemma (2.1) therefore implies that any root of $x^m - k$ is irrational. But $\sqrt[m]{k}$ is, by definition, a root of this polynomial, so it is irrational. ■

(b) Collaborate with your tablemates to write a clear, textbook quality proof of Lemma 2.1 on your whiteboard. (Besides clarity and correctness, textbook quality requires good English with proper punctuation. When a real textbook writer does this, it usually takes multiple revisions; if you're satisfied with your first draft, you're probably misjudging.) You may find it helpful to appeal to the following:

Lemma 2.2. *If a prime, p, is a factor of some power of an integer, then it is a factor of that integer.*

You may assume Lemma 2.2 without writing down its proof, but see if you can explain why it is true.

Solution. *Proof.* Let r be a real root of the polynomial, so that

$$a_0 + a_1 r + a_2 r^2 + \cdots + a_{m-1} r^{m-1} + r^m = 0.$$

There are three cases: either r is an integer, or r is irrational, or $r = s/t$ for integers s and t which have no common factors and such that $t > 1$. We want to eliminate the last case, so assume for the sake of contradiction that it held for some r.

Substituting s/t for r and multiplying both sides of the above equation by t^m yields:

$$a_0 t^m + a_1 s t^{m-1} + a_2 s^2 t^{m-2} + \cdots + a_{m-1} s^{m-1} t + s^m = 0, \tag{5}$$

$$a_0 t^m + a_1 s t^{m-1} + a_2 s^2 t^{m-2} + \cdots + s^{m-1} t = -s^m. \tag{6}$$

Now since $t > 1$, it must have a prime factor, p. The prime, p, therefore divides each term of the lefthand side of equation (6), so p also divides the righthand side, $-s^m$. This means that p divides s^m, so by Lemma 2.2, p is also a factor of s. So p is a common factor of s and t, contradicting the fact that s and t have no common factors. ■

Lemma 2.2 is a simple consequence of the *Fundamental Theorem of Arithmetic* which says that every integer > 1 factors into a product of primes that is *unique* except for the order in which the primes are multiplied.

For example, here are some ways to express 140 as a product of primes:

$$140 = 2 \cdot 2 \cdot 5 \cdot 7 = 2 \cdot 5 \cdot 7 \cdot 2 = 7 \cdot 5 \cdot 2 \cdot 2 = \cdots.$$

By the Fundamental Theorem, every such product will have exactly two occurrences of 2 and one each of 5 and 7. Next, we can obviously get a product of primes equal to, say, the third power of 140 by taking a product that equals 140 and repeating it three times. For example,

$$(140)^3 = 2 \cdot 2 \cdot 5 \cdot 7 \quad \cdot \quad 2 \cdot 2 \cdot 7 \cdot 5 \quad \cdot \quad 2 \cdot 2 \cdot 7 \cdot 5.$$

The Fundamental Theorem now says that *every* prime product equal to the third power of 60 must have the same primes as this repeated product, namely, six occurrences of 2 and three occurrences each of 5 and 7. In particular, the *only* primes that are factors of $(140)^3$ are the primes 2, 5 and 7 that are factors of 140. This reasoning applies equally well with any other integer greater than 1

in place of 140 and any power greater than 0 in place of 3, proving that if p is a prime factor of s^m, then p must have been a factor of s.

The Fundamental Theorem of Arithmetic is also know as the *Unique Prime Factorization Theorem*. It is one of those familiar mathematical facts that is not exactly obvious. We'll work out a proof of the Fundamental Theorem in a later chapter. ■

Problem 3.
If we raise an irrational number to an irrational power, can the result be rational? Show that it can by considering $\sqrt{2}^{\sqrt{2}}$ and arguing by cases.

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

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

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

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

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

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

■

Problem 4.
Here is a different proof that $\sqrt{2}$ is irrational, taken from the American Mathematical Monthly, v.116, #1, Jan. 2009, p.69:

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

(a) This proof was written for an audience of college teachers, and is a little more concise than desirable at this point in 6.042. Write out a more complete version which includes an explanation of each step.

Solution. The points that need justification are:

1. Why is there a positive integer, q, such that $\left(\sqrt{2}-1\right)q$ is a nonnegative integer? *Answer:* Since $\sqrt{2}$ is rational, so is $\sqrt{2}-1$. So $\sqrt{2}-1$ can be expressed as an integer quotient with positive denominator; now just let q be that denominator.
2. Why is there such a *least* positive integer, q? *Answer:* As long as there is one such positive integer, there has to be a least one. This obvious fact is known as the *Well Ordering Principle*.

3. Why is $0 < q' < q$? *Answer:* We know that $1 < \sqrt{2} < 2$, so $0 < \sqrt{2} - 1 < 1$. Therefore, $0 < \left(\sqrt{2} - 1\right) r < r$ for any real number $r > 0$.
4. Why is $(\sqrt{2}-1)q'$ a nonnegative integer? *Answer:* It's actually positive, because it is a product of positive numbers. It's integer because

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

and the last term is of the form $\langle \text{integer} - 2 \cdot [\text{integer}] \rangle$.

■

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

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

6.042J / 18.062J Mathematics for Computer Science
Spring 2010

Solutions to In-Class Problems Week 2, Mon.

Problem 1.
The proof below uses the Well Ordering Principle to prove that every amount of postage that can be paid exactly using only 6 cent and 15 cent stamps, is divisible by 3. Let the notation "$j \mid k$" indicate that integer j is a divisor of integer k, and let $S(n)$ mean that exactly n cents postage can be paid using only 6 and 15 cent stamps. Then the proof shows that

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

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

Let C be the set of *counterexamples* to (*), namely[1]

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

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

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

defines the set, C, of counterexamples. ■

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

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

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

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

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

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

[1]The notation "$\{n \mid \ldots\}$ means "the set of elements, n, such that ...."

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

Next suppose $S(m-15)$ holds. Then the proof for $m-6$ carries over directly for $m-15$ to yield a contradiction in this case as well. Since we get a contradiction in both cases, we conclude that...

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

which proves that (*) holds.

Problem 2.
Use the Well Ordering Principle to prove that

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

for all nonnegative integers, n.

Solution. The proof is by contradiction.

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

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

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

Now add m^2 to both sides of equation (2). Then the left hand side equals

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

and the right hand side equals

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

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

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

That is,

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

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

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

Here's the algebra:

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

■

Problem 3.
Euler's Conjecture in 1769 was that there are no positive integer solutions to the equation

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

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

Now let's consider Lehman's[2] equation, similar to Euler's but with some coefficients:

$$8a^4+4b^4+2c^4=d^4 \tag{3}$$

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

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

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

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

$$8a^4+4b^4+2c^4 \quad = \quad 16d'^4 \tag{4}$$

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

[2]Suggested by Eric Lehman, a former 6.042 Lecturer.

$$8a^4 + 4b^4 + 32c'^4 \quad = \quad 16d'^4 \tag{5}$$

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

$$8a^4 + 64b'^4 + 32c'^4 \quad = \quad 16d'^4 \tag{6}$$

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

6.042J / 18.062J Mathematics for Computer Science
Spring 2010

Solutions to In-Class Problems Week 2, Wed.

Problem 1.
Prove by truth table that OR distributes over AND:

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

Solution.

$[P$	OR	$(Q$	AND	$R)]$
T	T	T	T	T
T	T	T	F	F
T	T	F	F	T
T	T	F	F	F
F	T	T	T	T
F	F	T	F	F
F	F	F	F	T
F	F	F	F	F

$[(P$	OR	$Q)$	AND	$(P$	OR	$R)]$
T	T	T	T	T	T	T
T	T	T	T	T	T	F
T	T	F	T	T	T	T
T	T	F	T	T	T	F
F	T	T	T	F	T	T
F	T	T	F	F	F	F
F	F	F	F	F	T	T
F	F	F	F	F	F	F

The two columns for the principle operator (underlined) are the same, and therefore the corresponding propositional formulas are equivalent. ■

Problem 2.
This problem[1] examines whether the following specifications are *satisfiable*:

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

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

$$\begin{aligned} L &::= \text{file system locked,} \\ Q &::= \text{new messages are queued,} \\ B &::= \text{new messages are sent to the message buffer,} \\ N &::= \text{system functioning normally.} \end{aligned}$$

Solution. The translations of the specifications are:

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

■

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

Solution. An assignment that works is

$$\begin{aligned} L &= \text{True} \\ N &= \text{False} \\ Q &= \text{True} \\ B &= \text{False.} \end{aligned}$$

To find this assignment, we could have started constructing the sixteen line truth table —one line for each way of assigning truth values to the four variables L, N, Q, and B —and calculated the

[1] From Rosen, 5th edition, Exercise 1.1.36

truth value of the AND of all the five specifications under that assignment, continuing until we got one that made the AND-formula true.

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

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

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

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

Thus, in order for all five specifications to be true, the assignment must be:

$$\begin{aligned} L &= \text{True} \\ N &= \text{False} \\ Q &= \text{True} \\ B &= \text{False.} \end{aligned}$$

■

Problem 3.
When the Mathematician says to his student, "If a function is not continuous, then it is not differentiable," then letting D stand for "differentiable" and C for continuous, the only proper translation of the Mathematician's statement would be

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

or equivalently,

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

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

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

or equivalently,

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

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

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

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

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

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

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

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

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

■

Problem 4.
Propositional logic comes up in digital circuit design using the convention that **T** corresponds to 1 and **F** to 0. A simple example is a 2-bit half-adder circuit. This circuit has 3 binary inputs, a_1, a_0 and b, and 3 binary outputs, c, o_1, o_0. The 2-bit word a_1a_0 gives the binary representation of an integer, s between 0 and 3. The 3-bit word co_1o_0 gives the binary representation of $s + b$. The output c is called the *final carry bit*.

So if s and b were both 1, then the value of a_1a_0 would be `01` and the value of the output co_1o_0 would `010`, namely, the 3-bit binary representation of $1 + 1$.

In fact, the final carry bit equals 1 only when all three binary inputs are 1, that is, when $s = 3$ and $b = 1$. In that case, the value of co_1o_0 is `100`, namely, the binary representation of $3 + 1$.

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

$$\begin{aligned}
c_0 &= b \\
o_0 &= a_0 \ \text{XOR} \ c_0 \\
c_1 &= a_0 \ \text{AND} \ c_0 && \text{the carry into column 1} \\
o_1 &= a_1 \ \text{XOR} \ c_1 \\
c_2 &= a_1 \ \text{AND} \ c_1 && \text{the carry into column 2} \\
c &= c_2.
\end{aligned}$$

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

Solution. The $n+1$-bit word $a_n \ldots a_1 a_0$ will be the binary representation of an integer, s, between 0 and $2^{n+1} - 1$. The circuit will have $n+2$ outputs $c, o_n, \ldots, o_1, o_0$ where the $n+2$-bit word $co_n \ldots o_1 o_0$ gives the binary representation of $s + b$.

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

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

■

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

Solution. Define

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

■

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

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

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

■

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

The Propositional Operations

P	NOT P
T	**F**
F	**T**

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

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

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

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

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

6.042J / 18.062J Mathematics for Computer Science
Spring 2010

Solutions to In-Class Problems Week 2, Fri.

Problem 1.
Set Formulas and Propositional Formulas.

(a) Verify that the propositional formula $(P \text{ AND } \text{NOT}(Q)) \text{ OR } (P \text{ AND } Q)$ is equivalent to P.

Solution. There is a simple verification by truth table with 4 rows which we omit.

There is also a simple cases argument: if Q is **T**, then the formula simplifies to $(P \text{ AND } \mathbf{F}) \text{ OR } (P \text{ AND } \mathbf{T})$ which further simplifies to $(\mathbf{F} \text{ OR } P)$ which is equivalent to P.

Otherwise, if Q is **F**, then the formula simplifies to $(P \text{ AND } \mathbf{T}) \text{ OR } (P \text{ AND } \mathbf{F})$ which is likewise equivalent to P. ■

(b) Use part (a) to prove that

$$A = (A - B) \cup (A \cap B)$$

for any sets, A, B, where

$$A - B ::= \{a \in A \mid a \notin B\}.$$

Solution. We need only show that the two sets have the same elements, that is x is in one set iff x is in the other set, for any x.

Let P be $x \in A$ and Q be $x \in B$. Then

$$\begin{array}{lll}
x \in (A - B) \cup (A \cap B) & & \\
\quad \text{iff} \quad x \in (A - B) \text{ OR } x \in (A \cap B) & & \text{(by def of } \cup) \\
\quad \text{iff} \quad (x \in A \text{ AND } \text{NOT}(x \in B)) \text{ OR } (x \in A \text{ AND } x \in B) & & \text{(by def of } \cap \text{ and } -) \\
\quad \text{iff} \quad (P \text{ AND } \text{NOT}(Q)) \text{ OR } (P \text{ AND } Q) & & \text{(by def of } P \text{ and } Q) \\
\quad \text{iff} \quad P & & \text{(by part (a))} \\
\quad \text{iff} \quad x \in A & & \text{(by def of } P).
\end{array}$$

■

Problem 2.
Subset take-away[1] is a two player game involving a fixed finite set, A. Players alternately choose nonempty subsets of A with the conditions that a player may not choose

- the whole set A, or

[1] From Christenson & Tilford, *David Gale's Subset Takeaway Game, American Mathematical Monthly, Oct. 1997*

- any set containing a set that was named earlier.

The first player who is unable to move loses the game.

For example, if A is $\{1\}$, then there are no legal moves and the second player wins. If A is $\{1, 2\}$, then the only legal moves are $\{1\}$ and $\{2\}$. Each is a good reply to the other, and so once again the second player wins.

The first interesting case is when A has three elements. This time, if the first player picks a subset with one element, the second player picks the subset with the other two elements. If the first player picks a subset with two elements, the second player picks the subset whose sole member is the third element. Both cases produce positions equivalent to the starting position when A has two elements, and thus leads to a win for the second player.

Verify that when A has four elements, the second player still has a winning strategy.[2]

Solution. There are way too many cases to work out by hand if we tried to list all possible games. But the elements of A all behave the same, so we can cut to a small number of cases using the fact that permuting around the elements of A in any game yields another possible game. We can do this by not mentioning specific elements of A, but instead using the *variables* a, b, c, d whose values will be the four elements of A.

We consider two cases for the move of the Player 1 when the game starts:

1. Player 1 chooses a one element or a three element subset. Then Player 2 should choose the complement of Player one's choice. The game then becomes the same as playing the $n = 3$ game on the three element set chosen in this first round, where we know Player 2 has a winning strategy.

2. Player 1 chooses a subset of 2 elements. Let a, b be these elements, that is, the first move is $\{a, b\}$. Player 2 should choose the complement, $\{c, d\}$, of Player 1's choice. We then have the following subcases:

   (a) Player 1's second move is a one element subset, $\{a\}$. Player 2 should choose $\{b\}$. The game is then reduced to the two element game on $\{c, d\}$ where Player 2 has a winning strategy.

   (b) Player 1's second move is a two element subset, $\{a, c\}$. Player 2 should choose its complement, $\{b, d\}$. This leads to two subsubcases:

      i. Player 1's third move is one of the remaining sets of size two, $\{a, d\}$. Player 2 should choose its complement, $\{b, c\}$. The remaining possible moves are the four sets of size 1, where the Player 2 clearly wins after two more rounds.

      ii. Player 1's third move is a one element set, $\{a\}$. Player 2 should choose $\{b\}$. The game is then reduced to the case two element game on $\{c, d\}$ where Player 2 has a winning strategy.

So in all cases, Player 2 has a winning strategy in the Gale game for $n = 4$. ■

[2] David Gale worked out some of the properties of this game and conjectured that the second player wins the game for any set A. This remains an open problem.

Problem 3.
Define a *surjection relation*, surj, on sets by the rule

Definition. A surj B iff there is a surjective **function** from A to B.

Define the *injection relation*, inj, on sets by the rule

Definition. A inj B iff there is a total injective *relation* from A to B.

(a) Prove that if A surj B and B surj C, then A surj C.

Solution. By definition of surj, there are surjective functions, $F : A \to B$ and $G : B \to C$.
Let $H ::= G \circ F$ be the function equal to the composition of G and F, that is

$$H(a) ::= G(F(a)).$$

We show that H is surjective, which will complete the proof. So suppose $c \in C$. Then since G is a surjection, $c = G(b)$ for some $b \in B$. Likewise, $b = F(a)$ for some $a \in A$. Hence $c = G(F(a)) = H(a)$, proving that c is in the range of H, as required. ■

(b) Explain why A surj B iff B inj A.

Solution. *Proof.* (right to left): By definition of inj, there is a total injective relation, $R : B \to A$. But this implies that R^{-1} is a surjective function from A to B.
(left to right): By definition of surj, there is a surjective function, $F : A \to B$. But this implies that F^{-1} is a total injective relation from A to B. ■

(c) Conclude from (a) and (b) that if A inj B and B inj C, then A inj C.

Solution. From (b) and (a) we have that if C inj B and B inj A, then C inj A, so just switch the names A and C. ■

6.042J / 18.062J Mathematics for Computer Science
Spring 2010

Solutions to In-Class Problems Week 3, Tue.

Problem 1.

Lemma 4.9.4. Let A be a set and $b \notin A$. If A is infinite, then there is a bijection from $A \cup \{b\}$ to A.

Proof. Here's how to define the bijection: since A is infinite, it certainly has at least one element; call it a_0. But since A is infinite, it has at least two elements, and one of them must not be equal to a_0; call this new element a_1. But since A is infinite, it has at least three elements, one of which must not equal a_0 or a_1; call this new element a_2. Continuing in the way, we conclude that there is an infinite sequence $a_0, a_1, a_2, \ldots, a_n, \ldots$ of different elements of A. Now we can define a bijection $f : A \cup \{b\} \to A$:

$$\begin{aligned} f(b) &::= a_0, \\ f(a_n) &::= a_{n+1} && \text{for } n \in \mathbb{N}, \\ f(a) &::= a && \text{for } a \in A - \{b, a_0, a_1, \ldots\}. \end{aligned}$$

■

(a) Several students felt the proof of Lemma 4.9.4 was worrisome, if not circular. What do you think?

Solution. There is no "solution" for this discussion problem, since it depends on what seems bothersome.

It may be bothersome that the proof asserts that f is bijection without spelling out a proof. But the bijection property really does follow directly from definition of f, so it shouldn't be much burden for a bothered reader to fill in such a proof.

Another possibly bothersome point is that the proof assumes that if a set is infinite, it must have more than n elements, for every nonnegative integer n. But really that's the definition of infinity: a set is finite iff it has n elements for some nonnegative integer, n, and a set is infinite iff it is *not* finite.

A possibly worrisome point is how you find an element $a_{n+1} \in A$ given $a_0, a_1, \ldots, a_n$. But you don't have to *find* a specific one: there must be an element in $A - \{a_0, a_1, \ldots, a_n\}$ —so just pick any one. Actually, the justification for this step is the set-theoretic Axiom of Choice described in the Notes chapter first-order logic, and some logicians do consider it worrisome. ■

(b) Use the proof of Lemma 4.9.4 to show that if A is an infinite set, then there is surjective function from A to $\mathbb{N}$, that is, every infinite set is "as big as" the set of nonnegative integers.

Solution. By the proof of Lemma 4.9.4, there is an infinite sequence $a_0, a_1, a_2, \ldots, a_n, \ldots$ of different elements of A. Then we can define a surjective function $f : A \to \mathbb{N}$ by defining

$$f(a) ::= \begin{cases} n, & \text{if } a = a_n, \\ \text{undefined}, & \text{otherwise.} \end{cases}$$

—A total surjective function is not required, but if you want one define $f' : A \to \mathbb{N}$, by

$$f'(a) ::= \begin{cases} n, & \text{if } a = a_n, \\ 0, & \text{otherwise.} \end{cases}$$

■

Problem 2.
Let $R : A \to B$ be a binary relation. Use an arrow counting argument to prove the following generalization of the Mapping Rule:

Lemma. *If R is a function, and $X \subseteq A$, then*

$$|X| \geq |XR|.$$

Solution. *Proof.* The proof is virtually a repeat of the proof in the Appendix for the first Mapping Rule.

Since R is a function, the number of arrows whose starting point is an element of X is at most the number of elements in X, That is,

$$|X| \geq \#\text{arrows from } X.$$

Also, each element of XR is, by definition, the endpoint of at least one arrow starting from X, so there must be at least as many arrows starting from X as the number of elements of XR. That is,

$$\#\text{arrows from } X \geq |XR|.$$

Combining these inequalities immediately implies that $|X| \geq |XR|$. ■

An alternative proof appeals to the original Mapping Rule:

Proof. Consider the relation R' whose domain is X, whose codomain is XR, and whose arrows are just the arrows of R that start from X. (These arrows necessarily end in XR by definition of XR.) Since R is a function, R' will be one too, and by definition of XR, the relation R' is a surjection. Hence the first Mapping Rule implies that $|X| \geq |XR|$. ■

Problem 3.
Let $A = \{a_0, a_1, \ldots, a_{n-1}\}$ be a set of size n, and $B = \{b_0, b_1, \ldots, b_{m-1}\}$ a set of size m. Prove that $|A \times B| = mn$ by defining a simple bijection from $A \times B$ to the nonnegative integers from 0 to $mn - 1$.

Solution. A bijection $f : A \times B \to \{0, 1, \ldots, mn - 1\}$ can be defined by the rule

$$f(a_k, b_j) ::= jn + k.$$

■

Problem 4.
The rational numbers fill in all the spaces between the integers, so a first thought is that there must be more of them than the integers, but it's not true. In this problem you'll show that there are the same number of nonnegative rational as nonnegative integers. In short, the nonnegative rationals are countable.

(a) Describe a bijection between all the integers, $\mathbb{Z}$, and the nonnegative integers, $\mathbb{N}$.

Solution. One such bijection is defined by lining up all the integers and the nonnegative integers as follows:

$$\begin{array}{cccccccccc} 0 & 1 & -1 & 2 & -2 & 3 & -3 & 4 & \ldots \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & \ldots \end{array}$$

We can also define this bijection, $f : \mathbb{Z} \to \mathbb{Z}^+$, by a specification rule

$$f(n) = \begin{cases} -2n & \text{for } n \leq 0, \\ 2\,|n| - 1 & \text{for } n > 0. \end{cases}$$

■

(b) Define a bijection between the nonnegative integers and the set, $\mathbb{N} \times \mathbb{N}$, of all the ordered pairs of nonnegative integers:

$$\begin{array}{l} (0,0), (0,1), (0,2), (0,3), (0,4), \ldots \\ (1,0), (1,1), (1,2), (1,3), (1,4), \ldots \\ (2,0), (2,1), (2,2), (2,3), (2,4), \ldots \\ (3.0), (3,1), (3,2), (3,3), (3,4), \ldots \\ \quad \vdots \end{array}$$

Solution. Line up all the pairs by following successive upper-right to lower-left diagonals along the top row.

That is, start with (0,0) which counts as an initial diagonal of length 1. Then follow the length 2 second diagonal (0,1), (1,0), then the length 3 third diagonal (0,2), (1,1), (2,0), then the length 4 fourth diagonal (0,3), (1,2), (2,1), (3,0), ... So the line up would be

$$\begin{array}{cccccccccc} (0,0) & (0,1) & (1,0) & (0,2) & (1,1) & (2,0) & (0,3) & (1,2) & (2,1) & (3,0) & \ldots \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & \ldots \end{array}$$

It's interesting that this bijection from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{N}$ has a simple formula: the pair (k, m) is the kth element on the diagonal consisting of the pairs whose sum is $k + m$. The total number of elements in all the preceding diagonals is

$$0 + 1 + 2 + \cdots + (k + m) = (k + m + 1)(k + m)/2$$

so the pair (k, m) appears as the $(k + m + 1)(k + m)/2 + k$th element in the line up. ■

(c) Conclude that $\mathbb{N}$ is the same size as the set, $\mathbb{Q}$, of all nonnegative rational numbers.

Solution. One way to line up the nonnegative rationals is to take the list of all pairs, (k, m), of integers above and replace each remaining pair by the rational number k/m, skipping the pairs where $m = 0$:

$$0/1 \;\; 0/2 \;\; 1/1 \;\; 1/2 \;\; 0/3 \;\; 1/2 \;\; 2/1 \;\; 0/3 \;\; 1/2 \;\; 2/1 \;\; \ldots$$

and, going from left to right, delete all the occurrences of numbers that are already in the list:

$$0 \;\; 1 \;\; 1/2 \;\; 2 \;\; 3 \;\; 1/3 \;\; 1/4 \ldots.$$

■

6.042J / 18.062J Mathematics for Computer Science
Spring 2010

Solutions to In-Class Problems Week 3, Wed.

Problem 1.
For each of the logical formulas, indicate whether or not it is true when the domain of discourse is $\mathbb{N}$ (the nonnegative integers 0, 1, 2, ...), $\mathbb{Z}$ (the integers), $\mathbb{Q}$ (the rationals), $\mathbb{R}$ (the real numbers), and $\mathbb{C}$ (the complex numbers).

$$\begin{array}{rlrcl} & \exists x & (x^2 & = & 2) \\ \forall x & \exists y & (x^2 & = & y) \\ \forall y & \exists x & (x^2 & = & y) \\ \forall x \neq 0 & \exists y & (xy & = & 1) \\ \exists x & \exists y & (x+2y & = & 2) \wedge (2x+4y=5) \end{array}$$

Solution.

Statement	$\mathbb{N}$	$\mathbb{Z}$	$\mathbb{Q}$	$\mathbb{R}$	$\mathbb{C}$
$\exists x\ (x^2 = 2)$	F	F	F	$T\ (x = \sqrt{2})$	T
$\forall x \exists y\ (x^2 = y)$	T	T	T	$T\ (y = x^2)$	t
$\forall y \exists x\ (x^2 = y)$	F	F	F	F (take $y < 0$)	t
$\forall x \neq 0 \exists y\ (xy = 1)$	F	F	T	$T\ (y = 1/x)$	T
$\exists x \exists y\ (x + 2y = 2) \wedge (2x + 4y = 5)$	F	F	F	F	F

■

Problem 2.
The goal of this problem is to translate some assertions about binary strings into logic notation. The domain of discourse is the set of all finite-length binary strings: λ, 0, 1, 00, 01, 10, 11, 000, 001, ... (Here λ denotes the empty string.) In your translations, you may use all the ordinary logic symbols (including =), variables, and the binary symbols `0`, `1` denoting 0, 1.

A string like `01`x`0`y of binary symbols and variables denotes the *concatenation* of the symbols and the binary strings represented by the variables. For example, if the value of x is `011` and the value of y is `1111`, then the value of `01`x`0`y is the binary string `0101101111`.

Here are some examples of formulas and their English translations. Names for these predicates are listed in the third column so that you can reuse them in your solutions (as we do in the definition of the predicate NO-1S below).

Meaning	Formula	Name
x is a prefix of y	$\exists z\ (xz = y)$	PREFIX(x, y)
x is a substring of y	$\exists u \exists v\ (uxv = y)$	SUBSTRING(x, y)
x is empty or a string of 0's	NOT(SUBSTRING$(1, x)$)	NO-1S(x)

(a) x consists of three copies of some string.

Solution. $\exists y\ (x = yyy)$

■

(b) x is an even-length string of 0's.

Solution. NO-1S$(x) \wedge \exists y\ (x = yy)$

■

(c) x does not contain both a 0 and a 1.

Solution. NOT[SUBSTRING$(0, x)$ AND SUBSTRING$(1, x)$]

■

(d) x is the binary representation of $2^k + 1$ for some integer $k \geq 0$.

Solution. $(x = 10)$ OR $(\exists y\ (x = 1y1$ AND NO-1S$(y)))$ ■

(e) An elegant, slightly trickier way to define NO-1S(x) is:

$$\text{PREFIX}(x, 0x). \qquad \text{(*)}$$

Explain why (*) is true only when x is a string of 0's.

Solution. Prefixing x with 0 rightshifts all the bits. So the nth symbol of x shifts into the $(n+1)$st symbol of $0x$. Now for x to be a prefix of $0x$, the $n+1$st symbol of $0x$ must match the $(n+1)$st symbol of x. So if x satisfies (*), the nth and $(n+1)$st symbols of x must match. This holds for all $n > 0$ up to the length of x, that is, *all* the symbols of x must be the same. In addition, if $x \neq \lambda$, it must start with 0. Therefore, if x satisfies (*), all its symbols must be 0's.

Note that it's easy to see, conversely, that if $x = \lambda$ or x is all 0's, then of course it satisfies (*). ■

6.042J / 18.062J Mathematics for Computer Science
Spring 2010

Solutions to In-Class Problems Week 3, Fri.

Problem 1.
Let's refer to a programming procedure (written in your favorite programming language —C++, or Java, or Python, ...) as a *string procedure* when it is applicable to data of type `string` and only returns values of type `boolean`. When a string procedure, P, applied to a `string`, s, returns **True**, we'll say that P *recognizes* s. If $\mathcal{R}$ is the set of strings that P recognizes, we'll call P a *recognizer* for $\mathcal{R}$.

(a) Describe how a recognizer would work for the set of strings containing only lower case Roman letter —`a`, `b`, ..., `z` —such that each letter occurs twice in a row. For example, `aaccaabbzz`, is such a string, but `abb`, `00bb`, `AAbb`, and `a` are not. (Even better, actually write a recognizer procedure in your favorite programming language).

Solution. All the standard programming languages have built-in operations for scanning the characters in a string. So simply write a procedure that checks an input string left to right, verifying that successive pairs of characters in the string are duplicated, lowercase roman characters.

ACTUAL PROGRAM TBA

■

A set of `strings` is called *recognizable* if there is a recognizer procedure for it.

When you actually program a procedure, you have to type the program text into a computer system. This means that every procedure is described by some `string` of typed characters. If a `string`, s, is actually the typed description of some string procedure, let's refer to that procedure as P_s. You can think of P_s as the result of compiling s.[1]

In fact, it will be helpful to associate every string, s, with a procedure, P_s; we can do this by defining P_s to be some fixed string procedure —it doesn't matter which one —whenever s is not the typed description of an actual procedure that can be applied to `string` s. The result of this is that we have now defined a total function, f, mapping every `string`, s, to the set, $f(s)$, of `strings` recognized by P_s. That is we have a total function,

$$f : \texttt{string} \to \mathcal{P}(\texttt{string}). \tag{1}$$

(b) Explain why the actual range of f is the set of all recognizable sets of strings.

[1] The string, s, and the procedure, P_s, have to be distinguished to avoid a type error: you can't apply a string to string. For example, let s be the string that you wrote as your program to answer part (a). Applying s to a string argument, say `oorrmm`, should throw a type exception; what you need to do is apply the procedure P_s to `oorrmm`. This should result in a returned value **True**, since `oorrmm` consists of three pairs of lowercase roman letters

Solution. Since $f(s)$ is the set of strings recogized by P_s, everything in range (f) is a recogizable set. Conversely, every recogizable set is in range (f): if $\mathcal{R}$ is a recognizable set, then by definition, there is a procedure, P, that recognizes R. So if r is the input program from which P was compiled, then $\mathcal{R} = f(r)$. ■

This is exactly the set up we need to apply the reasoning behind Russell's Paradox to define a set that is not in the range of f, that is, a set of strings, $\mathcal{N}$, that is *not* recognizable.

(c) Let

$$\mathcal{N} ::= \{s \in \texttt{string} \mid s \notin f(s)\}.$$

Prove that $\mathcal{N}$ is not recognizable.

Hint: Similar to Russell's paradox or the proof of Theorem **??**.

Solution. By definition of $\mathcal{N}$,

$$s \in \mathcal{N} \quad \text{iff} \quad s \notin f(s). \tag{2}$$

for every `string`, s.

Now assume to the contrary that $\mathcal{N}$ was recognizable by some string procedure. This procedure must have a string, w, that describes it, so we have

$$\begin{aligned} s \in \mathcal{N} \quad &\text{iff} \quad P_w \text{ applied to } s \text{ returns } \textbf{True}, \\ &\text{iff} \quad s \in f(w) \qquad\qquad \text{(by def. of } f\text{)} \end{aligned} \tag{3}$$

for all `string`'s s.

Combining (2) and (3), we have that for every string, s,

$$s \notin f(s) \quad \text{iff} \quad s \in f(w), \tag{4}$$

for all `string`'s s.

Now letting s be w in (4), we reach the contradiction

$$w \notin f(w) \quad \text{iff} \quad w \in f(w).$$

This contradiction implies that the assumption that $\mathcal{N}$ was recognizable must be false.

■

(d) Discuss what the conclusion of part (c) implies about the possibility of writing "program analyzers" that take programs as inputs and analyze their behavior.

Solution. Let's call a programming procedure "self-unconscious" if it does not return **True** when applied to its own textual definition.

Rephrased informally, the conclusion of part (c) says that it is logically impossible to design a *general* program analyzer, which takes as input the (textual definition) of an arbitrary program, and recognizes when the program is self-unconscious. This implies that it is impossible to write a program which does the more general analysis of how an arbitrary procedure behaves when applied to some given arguments.

BTW, it *is* feasible to write a general procedure that recognizes when an arbitrary input procedure *does* return a value when appiled to the string that describes it —that is, when the procedure is *self-conscious*. The general procedure appllied to input s just simulates P_s applied to s. In other words, this general procedure just acts like a virtual machine simulator or "interpreter" for the programming language of its input programs.

It's also important to recognize that there's no hope of getting around this by switching programming languages. For example, by part (c), no C++ program can analyze arbitrary C++ programs, and no Java program can analyze Java programs, but you might wonder if a language like C++, which allows more intimate manipulation of computer memory than Java, might therefore allow a C++ program to analyze general Java programs. But there is no loophole here: since it's possible to write a Java program that is a simulator/interpreter for C++ programs, if a C++ program could analyze Java programs, so could the Java program that simulated the C++ program, contradicting (c).

It's a different story if we think about the *practical* possibility of writing programming analyzers. The fact that it's logically impossible to write analyzers for completely general programs does not mean that you can't do a very good job analyzing interesting programs that come up in practice. In fact these "interesting" programs are commonly *intended* to be analyzable in order to confirm that they do what they're supposed to do.

So it's not clear how much of a hurdle this theoretical limitation implies in practice. What the theory does provide is some perspective on claims about general analysis methods for programs. The theory tells us that people who make such claims either

- are exaggerating the power (if any) of their methods —say to get a grant or make a sale, or
- are trying to keep things simple by not going into technical limitations they're aware of, or
- perhaps most commonly, are so excited about some useful practical successes of their methods, that they haven't bothered to think about their limitations.

So from now on, if you hear people making claims about completely general program analysis/verification/optimization methods, you'll know they can't be telling the whole story. ■

Problem 2.
The Axiom of Choice can say that if s is a set whose members are nonempty sets that are *pairwise disjoint* —that is no two sets in s have an element in common —then there is a set, c, consisting of exactly one element from each set in s.

In formal logic, we could describe s with the formula,

$$\text{pairwise-disjoint}(s) ::= \quad \forall x \in s.\, x \neq \emptyset QAND \forall x, y \in s.(x \neq y) \text{ IMPLIES } (x \cap y = \emptyset).$$

Similarly we could describe c with the formula

$$\text{choice-set}(c, s) ::= \quad \forall x \in s.\, \exists! z.\, z \in c \cap x.$$

Here "$\exists! z.$" is fairly standard notation for "there exists a *unique* z.

Now we can give the formal definition:

Definition (Axiom of Choice)**.**

$$\forall s.\, \text{pairwise-disjoint}(s) \text{ IMPLIES } \exists c.\, \text{choice-set}(c, s).$$

The only issue here is that Set Theory is technically supposed to be expressed in terms of *pure* formulas in the language of sets, which means formula that uses only the membership relation, $\in$, propositional connectives, and the two quantifies $\forall$ and $\exists$. Verify that the Axiom of Choice can be expressed as a pure formula, by explaining how to replace all impure subformulas above with equivalent pure formulas.

For example, the formula $x = y$ could be replaced with the pure formula $\forall z.\, z \in x \text{ IFF } z \in y$.

Solution. Here is how the impure subformulas used in the above definition of the Axiom of Choice can be translated into pure formulas:

$$x \neq \emptyset translates into \exists y / \, y \in x.$$

$$[x \cap y = \emptyset] translates into \, \text{NOT}(\exists z.\, z \in x \text{ AND } z \in y).$$

$$[z \in x \cap y] translates into z \in x \text{ AND } z \in y.$$

$$\exists! z.\, P(z) translates into \exists z.\, P(z) \text{ AND } \forall w.\, P(w) \text{ IMPLIES } w = z.$$

This last formula is not pure because it uses $=$, but this is ok since we know it can be replaced by a pure formula.

■

Problem 3.
There are lots of different sizes of infinite sets. For example, starting with the infinite set, $\mathbb{N}$, of nonnegative integers, we can build the infinite sequence of sets

$$\mathbb{N},\ \mathcal{P}(\mathbb{N}),\ \mathcal{P}(\mathcal{P}(\mathbb{N})),\ \mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbb{N}))),\ \ldots.$$

By Theorem **??** from the Notes, each of these sets is *strictly bigger*[2] than all the preceding ones. But that's not all: if we let U be the union of the sequence of sets above, then U is strictly bigger than every set in the sequence! Prove this:

Lemma. *Let $\mathcal{P}^n(\mathbb{N})$ be the nth set in the sequence, and*

$$U ::= \bigcup_{n=0}^{\infty} \mathcal{P}^n(\mathbb{N}).$$

Then

[2]Reminder: set A is *strictly bigger* than set B just means that A surj B, but NOT(B surj A).

1. $U \text{ surj } \mathcal{P}^n(\mathbb{N})$ *for every* $n \in \mathbb{N}$, *but*
2. *there is no* $n \in \mathbb{N}$ *for which* $\mathcal{P}^n(\mathbb{N}) \text{ surj } U$.

Now of course, we could take $U, \mathcal{P}(U), \mathcal{P}(\mathcal{P}(U)), \ldots$ and can keep on indefinitely building still bigger infinities.

Solution. Everything follows from a trivial observation: if $A \supseteq B$, then $A \text{ surj } B$. (Why is this trivial?)

So since $U \supseteq \mathcal{P}^n(\mathbb{N})$, we have $U \text{ surj } \mathcal{P}^n(\mathbb{N})$, which proves 1.

To prove 2, assume to the contrary that $\mathcal{P}^m(\mathbb{N}) \text{ surj } U$. Now we know from 1 that $U \text{ surj } \mathcal{P}^{m+1}(\mathbb{N})$. But this implies that

$$\mathcal{P}^m(\mathbb{N}) \text{ surj } \mathcal{P}^{m+1}(\mathbb{N}) = \mathcal{P}(\mathcal{P}^m(\mathbb{N})),$$

contradicting the fact that, by Theorem **??**, a power set of $\mathcal{P}^m(\mathbb{N}))$ is "strictly bigger" than $\mathcal{P}^m(\mathbb{N}))$. ■

6.042J / 18.062J Mathematics for Computer Science
Spring 2010

Solutions to In-Class Problems Week 4, Mon.

Problem 1.
Prove by induction:

$$1 + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{n^2} < 2 - \frac{1}{n}, \tag{1}$$

for all $n > 1$.

Solution. *Proof.* (By Induction). The induction hypothesis is $P(n)$ is the inequality (1).

Base Case: ($n = 2$). The LHS of(1) in this case is $1 + 1/4$ and the RHS is $2 - 1/2$. Since LHS $= 5/4 < 6/4 = 3/2 =$ RHS, inequality (1) holds, and $P(2)$ is proved.

Inductive Step: Let n be any natural number greater than 1, and assume $P(n)$ in order to prove $P(n+1)$. That is, we assume (1) Adding $1/(n+1)^2$ to both sides of this inequality yields

$$\begin{aligned}
1 + \frac{1}{4} + \cdots + \frac{1}{n^2} + \frac{1}{(n+1)^2} &< 2 - \frac{1}{n} + \frac{1}{(n+1)^2} \\
&= 2 - \left(\frac{1}{n} - \frac{1}{(n+1)^2}\right) \\
&= 2 - \left(\frac{n^2 + 2n + 1 - n}{n(n+1)^2}\right) \\
&= 2 - \frac{n^2 + n}{n(n+1)^2} - \frac{1}{n(n+1)^2} \\
&= 2 - \frac{1}{n+1} - \frac{1}{n(n+1)^2} \\
&< 2 - \frac{1}{n+1}.
\end{aligned}$$

So we have proved $P(n+1)$. ■

Problem 2. (a) Prove by induction that a $2^n \times 2^n$ courtyard with a 1×1 statue of Bill in *a corner* can be covered with L-shaped tiles. (Do not assume or reprove the (stronger) result of Theorem 6.1.2 that Bill can be placed anywhere. The point of this problem is to show a different induction hypothesis that works.)

Solution. Let $P(n)$ be the proposition Bill can be placed in a corner of a $2^n \times 2^n$ courtyard with a proper tiling of the remainder with L-shaped tiles.

Base case: $P(0)$ is true because Bill fills the whole courtyard.

Inductive step: Assume that $P(n)$ is true for some $n \geq 0$; that is, there exists a tiling of the $2^n \times 2^n$ courtyard leaving Bill in a corner.

To prove, $P(n+1)$, Divide the $2^{n+1} \times 2^{n+1}$ courtyard into four quadrants, each $2^n \times 2^n$. One quadrant will contain the corner designated for Bill. By induction hypothesis, we can get Bill into some corner of the quadrant, which means we can actually get him into *any* desired corner of the quadrant by rotating the tiling of the quadrant. So place Bill in the designated corner of the quandrant, and tile the rest of the quadrant.

Now tile the remaining three quadrants, leaving a tile space open in the quadrant corners that are in the middle of the whole $2^{n+1} \times 2^{n+1}$ courtyard (as in the diagram in the proof of Theorem 6.1.2). These three spaces form an L-shape that that can be filled with a single L-shaped tile, completing the full courtyard tiling. This proves $P(n+1)$, completing the proof by induction that a square courtyard with side length any power of 2 can be tiled with Bill in a corner.

■

(b) Use the result of part (a) to prove the original claim that there is a tiling with Bill in the middle.

Solution. To put Bill in the middle, tile each of the four quadrants, leaving the empty corner of the quadrant in the middle of the full courtyard. This leaves the four central squares of the full courtyard empty, so fill three of these squares with an L-shaped tile. This leaves a single central square untiled for Bill. ■

Problem 3.
Find the flaw in the following bogus proof that $a^n = 1$ for all nonnegative integers n, whenever a is a nonzero real number.

Bogus proof. The proof is by induction on n, with hypothesis

$$P(n) ::= \forall k \leq n.\, a^k = 1,$$

where k is a nonnegative integer valued variable.

Base Case: $P(0)$ is equivalent to $a^0 = 1$, which is true by definition of a^0. (By convention, this holds even if $a = 0$.)

Inductive Step: By induction hypothesis, $a^k = 1$ for all $k \in \mathbb{N}$ such that $k \leq n$. But then

$$a^{n+1} = \frac{a^n \cdot a^n}{a^{n-1}} = \frac{1 \cdot 1}{1} = 1,$$

which implies that $P(n+1)$ holds. It follows by induction that $P(n)$ holds for all $n \in \mathbb{N}$, and in particular, $a^n = 1$ holds for all $n \in \mathbb{N}$.

■

Solution. The flaw comes in the inductive step, where we implicitly assume $n \geq 1$ in order to talk about a^{n-1} in the denominator (otherwise the exponent is not a nonnegative integer, so we cannot apply the inductive hypothesis). We checked the base case only for $n = 0$, so we are not justified in assuming that $n \geq 1$ when we try to prove the statement for $n+1$ in the inductive step. And of course the proposition first breaks precisely at $n = 1$. ■

Problem 4.
Define the *potential*, $p(S)$, of a stack of blocks, S, to be $k(k-1)/2$ where k is the number of blocks in S. Define the potential, $p(A)$, of a set of stacks, A, to be the sum of the potentials of the stacks in A.

Generalize Theorem 6.2.2 about scores in the stacking game to show that for any set of stacks, A, if a sequence of moves starting with A leads to another set of stacks, B, then $p(A) \geq p(B)$, and the score for this sequence of moves is $p(A) - p(B)$.

Hint: Try induction on the number of moves to get from A to B.

Solution. *Proof.* The proof is by ordinary induction on the number of moves, n. The induction hypothesis will be

> $P(n)$::= If n moves from a set of stacks, A, leads to a set B of stacks, then $p(A) \geq p(B)$ and the score for these n moves is $p(A) - p(B)$.

Base case: (n = 0) This means no moves have been made and $B = A$, so it's obvious that $P(0)$ holds.

Inductive step: Assume that $P(n)$ is true for some $n \in \mathbb{N}$, and suppose A leads to B in $n+1$ moves. This means that A leads to some set of stacks, A_1, and A_1 leads to B in n steps. So the inductive hypothesis $P(n)$ implies that $p(A_1) \geq p(B)$ and the score for going from A_1 to B is $p(A_1) - p(B)$.

So all we have to do is show that the score for the single move from A to A_1 is $p(A) - p(A_1) > 0$. The only difference between A and A_1 is that some stack $S \in A$ of size $k > 1$ splits into two stacks of sizes $k_1, k_2 \geq 1$ where $k = k_1 + k_2$. The score for such a move is $k_1 k_2$. Also,

$$p(S) = \frac{(k_1 + k_2)((k_1 + k_2) + 1)}{2} = \frac{(k_1^2 + 2k_1k_2 + k_2^2) + (k_1 + k_2)}{2},$$

and the potential of the two stack sets is the sum of their potentials, namely,

$$\frac{k_1(k_1 + 1) + k_2(k_2 + 1)}{2} = \frac{k_1^2 + k_2^2 + k_1 + k_2}{2},$$

So the difference between these potentials equals $k_1 k_2 > 0$, and this is indeed equal to the score of the move.

■

6.042J / 18.062J Mathematics for Computer Science
Spring 2010

Solutions to In-Class Problems Week 4, Wed.

Problem 1.

Direct Prerequisites	Subject
18.01	6.042
18.01	18.02
18.01	18.03
8.01	8.02
8.01	6.01
6.042	6.046
18.02, 18.03, 8.02, 6.01	6.02
6.01, 6.042	6.006
6.01	6.034
6.02	6.004

(a) For the above table of MIT subject prerequisites, draw a diagram showing the subject numbers with a line going down to every subject from each of its (direct) prerequisites.

Solution.

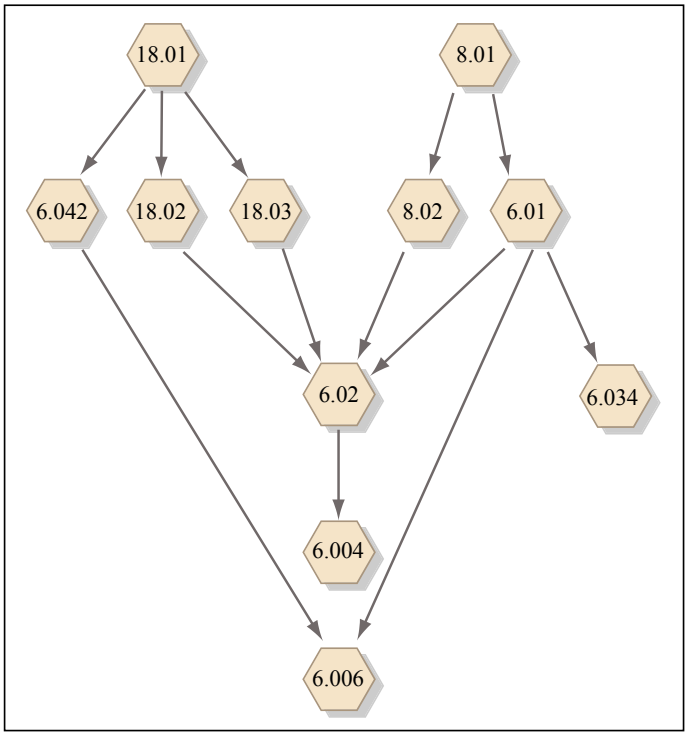


Image by MIT OpenCourseWare. ■

(b) Give an example of a collection of sets partially ordered by the proper subset relation, $\subset$, that is isomorphic to ("same shape as") the prerequisite relation among MIT subjects from part (a).

Solution. For each subject, S, let

$$\text{preset}(S) ::= \{S' \mid S' \text{ is an indirect prerequisite of } S \text{ OR } S' = S\}.$$

For example,

subject	preset
18.02	$\{18.01, 18.02\}$
18.03	$\{18.01, 18.03\}$
6.006	$\{6.042, 18.01, 6.01, 8.01, 6.006\}$

Note that the "OR$S = S'$" clause is necessary: if we let the set representing subject S just be the indirect prerequisites of S, then 18.02 and 18.03, for example, would be represented by the same set, $\{18.01\}$. Then the correspondence between subjects and sets would no longer be a bijection, which is a requirement for isomporphism.

■

(c) Explain why the empty relation is a strict partial order and describe a collection of sets partially ordered by the proper subset relation that is isomorphic to the empty relation on five elements —that is, the relation under which none of the five elements is related to anything.

Solution. An empty relation is always a partial order: it is *vacuously* asymmetric and transitive. It's not weak because it is not reflexive; in fact it's irreflexive.

Letting the five elements be $1, 2, 3, 4, 5$, the recipe of mapping an element to its preimages under the relation, with the element itself thrown in, gives the five sets $\{1\}, \{2\}, \{3\}, \{4\}, \{5\}$.

Of course any 5 sets none of which is contained in any of the others will also work, for example, all the size 4 subsets of $\{1, 2, 3, 4, 5\}$ ■

(d) Describe a *simple* collection of sets partially ordered by the proper subset relation that is isomorphic to the "properly contains" relation, $\supset$, on $\mathcal{P}\{1, 2, 3, 4\}$.

Solution. The standard inverse image solution involves sets of subsets. A more elegant correspondence is to let each set $A \subseteq \{1, 2, 3, 4\}$ correspond to its complement. That is,

$$f(A) = \overline{A} ::= \{1, 2, 3, 4\} - A.$$

This works because $A \supset B$ iff $\overline{A} \subset \overline{B}$

■

Problem 2.
A binary relation, R, on a set, A, is *irreflexive* iff NOT$(a\ R\ a)$ for all $a \in A$. Prove that if a binary relation on a set is transitive and irreflexive, then it is strict partial order.

Solution. *Proof.* Suppose R transitive and irreflexive. Since it is transitive, to check that it is a strict partial order, we need only verify that it is asymmetric.

To prove that it is asymmetric, suppose $a\ R\ b$ holds for some $a, b \in A$. We need to prove NOT$(b\ R\ a)$.

So assume to the contrary that $b\ R\ a$ holds. Then $a\ R\ b$ and $b\ R\ a$, so by transitivity, $a\ R\ a$, contradicting the fact that R is irreflexive. So $b\ R\ a$ does not hold, as claimed. ■

Problem 3.
How many binary relations are there on the set $\{0, 1\}$?

How many are there that are transitive?, ... asymmetric?, ... reflexive?, ... irreflexive?, ... strict partial orders?, ... weak partial orders?

Hint: There are easier ways to find these numbers than listing all the relations and checking which properties each one has.

Solution. There are $2^4 = 16$ such relations, since in any such relation there are four possible arrows between $\{0, 1\}$ and itself, each of which may or may not be there.

There are 3 **in**transitive transitive relations, because the only way transitivity can fail in a relation on two elements is when there is an arrow in both directions between the elements, but one or the other or both the elements are missing a *self-loop*, that is, an arrow that starts and ends at the element. So there are $13 = 16 - 3$ transitive relations.

There are 3 asymmetric relations. Asymmetry implies no self-loops, and at most one of the two possible arrows between 0 and 1. So the only 3 possibilities are no arrows, arrow from 0 to 1, arrow from 1 to 0.

There are 4 reflexive relations, because two of the four possible arrows (the self-loops) must be present, the remaining two arrows can be either present or not present, which yields 2^2 relations. There are 4 irreflexive relations for the same reason.

There are 3 strict partial orders, because the 3 asymmetric relations are all transitive.

There are 3 weak partial orders, because the 3 strict partial orders remain distinct after adding self-loops to both elements.

■

6.042J / 18.062J Mathematics for Computer Science
Spring 2010

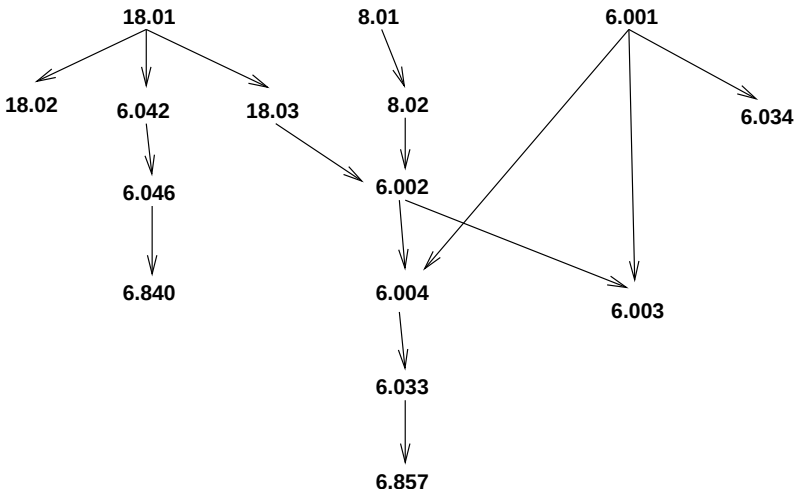
Solutions to In-Class Problems Week 4, Fri.

Problem 1.
The table below lists some prerequisite information for some subjects in the MIT Computer Science program (in 2006). This defines an indirect prerequisite relation, $\prec$, that is a strict partial order on these subjects.

$$\begin{aligned} 18.01 &\to 6.042 & 18.01 &\to 18.02 \\ 18.01 &\to 18.03 & 6.046 &\to 6.840 \\ 8.01 &\to 8.02 & 6.001 &\to 6.034 \\ 6.042 &\to 6.046 & 18.03, 8.02 &\to 6.002 \\ 6.001, 6.002 &\to 6.003 & 6.001, 6.002 &\to 6.004 \\ 6.004 &\to 6.033 & 6.033 &\to 6.857 \end{aligned}$$

(a) Explain why exactly six terms are required to finish all these subjects, if you can take as many subjects as you want per term. Using a *greedy* subject selection strategy, you should take as many subjects as possible each term. Exhibit your complete class schedule each term using a greedy strategy.

Solution. It helps to have a diagram of the direct prerequisite relation:



There is a $\prec$-chain of length six:

$$8.01 \prec 8.02 \prec 6.002 \prec 6.004 \prec 6.033 \prec 6.857$$

So six terms are necessary, because at most one of these subjects can be taken each term.

There is no longer chain, so with the greedy strategy you will take six terms. Here are the subjects you take in successive terms.

1:	6.001	8.01	18.01		
2:	6.034	6.042	8.02	18.02	18.03
3:	6.002	6.046			
4:	6.003	6.004	6.840		
5:	6.033				
6:	6.857				

■

(b) In the second term of the greedy schedule, you took five subjects including 18.03. Identify a set of five subjects not including 18.03 such that it would be possible to take them in any one term (using some nongreedy schedule). Can you figure out how many such sets there are?

Solution. We're looking for an antichain in the $\prec$ relation that does not include 18.03. Every such antichain will have to include 18.02, 6.003, 6.034. Then a fourth subject could be any of 6.042, 6.046, and 6.840. The fifth subject could then be any of 6.004, 6.033, and 6.857. This gives a total of nine antichains of five subjects. ■

(c) Exhibit a schedule for taking all the courses —but only one per term.

Solution. We're asking for a topological sort of $\prec$. There are many. One is 18.01, 8.01, 6.001, 18.02, 6.042, 18.03, 8.02, 6.034, 6.046, 6.002, 6.840, 6.004, 6.003, 6.033, 6.857. ■

(d) Suppose that you want to take all of the subjects, but can handle only two per term. Exactly how many terms are required to graduate? Explain why.

Solution. There are $\lceil 15/2 \rceil = 8$ terms necessary. The schedule below shows that 8 terms are sufficient as well:

1:	18.01	8.01
2:	6.001	18.02
3:	6.042	18.03
4:	8.02	6.034
5:	6.046	6.002
6:	6.840	6.004
7:	6.003	6.033
8:	6.857	

■

(e) What if you could take three subjects per term?

Solution. From part (a) we know six terms are required even if there is no limit on the number of subjects per term. Six terms are also sufficient, as the following schedule shows:

1:	18.01	8.01	6.001
2:	6.042	18.03	8.02
3:	18.02	6.046	6.002
4:	6.004	6.003	6.034
5:	6.840	6.033	
6:	6.857		

■

Problem 2.
A pair of 6.042 TAs, Liz and Oscar, have decided to devote some of their spare time this term to establishing dominion over the entire galaxy. Recognizing this as an ambitious project, they worked out the following table of tasks on the back of Oscar's copy of the lecture notes.

1. **Devise a logo** and cool imperial theme music - 8 days.
2. **Build a fleet** of Hyperwarp Stardestroyers out of eating paraphernalia swiped from Lobdell - 18 days.
3. **Seize control** of the United Nations - 9 days, after task #1.
4. **Get shots** for Liz's cat, Tailspin - 11 days, after task #1.
5. **Open a Starbucks chain** for the army to get their caffeine - 10 days, after task #3.
6. **Train an army** of elite interstellar warriors by dragging people to see *The Phantom Menace* dozens of times - 4 days, after tasks #3, #4, and #5.
7. **Launch the fleet** of Stardestroyers, crush all sentient alien species, and establish a Galactic Empire - 6 days, after tasks #2 and #6.
8. **Defeat Microsoft** - 8 days, after tasks #2 and #6.

We picture this information in Figure 1 below by drawing a point for each task, and labelling it with the name and weight of the task. An edge between two points indicates that the task for the higher point must be completed before beginning the task for the lower one.

(a) Give some valid order in which the tasks might be completed.

Solution. We can easily find several of them. The most natural one is valid, too: #1, #2, #3, #4, #5, #6, #7, #8.

■

Liz and Oscar want to complete all these tasks in the shortest possible time. However, they have agreed on some constraining work rules.

- Only one person can be assigned to a particular task; they can not work together on a single task.

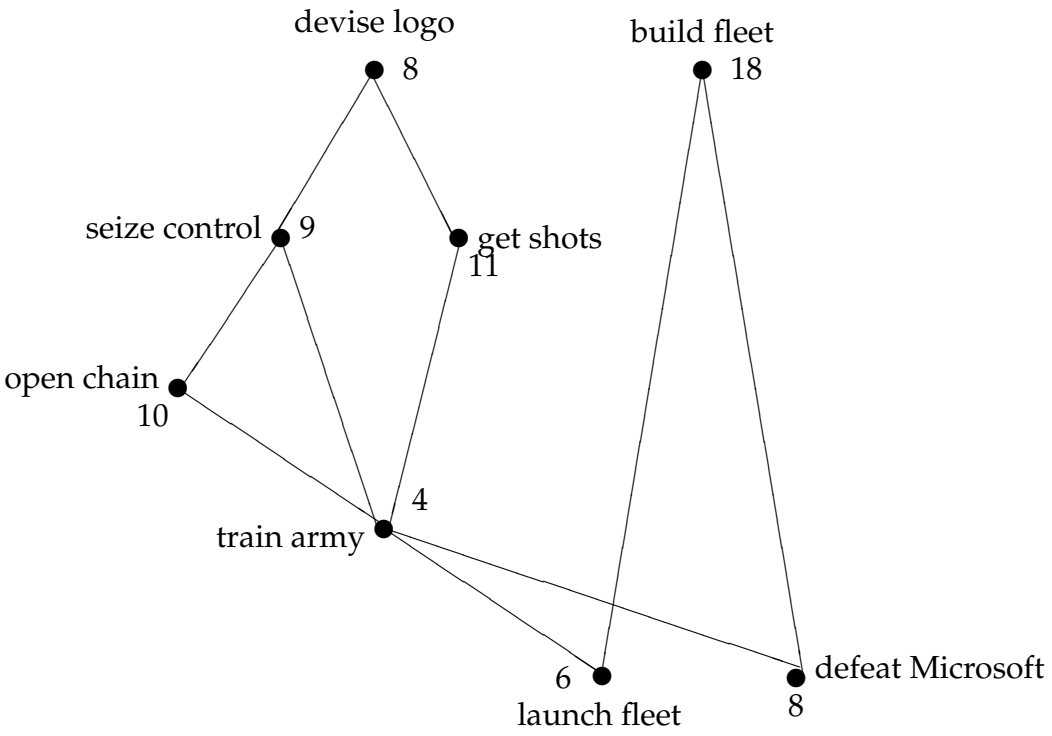


Figure 1: Graph representing the task precedence constraints.

- Once a person is assigned to a task, that person must work exclusively on the assignment until it is completed. So, for example, Liz cannot work on building a fleet for a few days, run to get shots for Tailspin, and then return to building the fleet.

(b) Liz and Oscar want to know how long conquering the galaxy will take. Oscar suggests dividing the total number of days of work by the number of workers, which is two. What lower bound on the time to conquer the galaxy does this give, and why might the actual time required be greater?

Solution.

$$\frac{8+18+9+11+10+4+6+8}{2} \quad = \quad 37 \text{ days}$$

If working together and interrupting work on a task were permitted, then this answer would be correct. However, the rules may prevent Liz and Oscar from both working all the time. For example, suppose the only task was building the fleet. It will take 18 days, not 18/2 days, to complete, because only one person can work on it and the other must sit idle. ■

(c) Liz proposes a different method for determining the duration of their project. He suggests looking at the duration of the "critical path", the most time-consuming sequence of tasks such that each depends on the one before. What lower bound does this give, and why might it also be too low?

Solution. The longest sequence of tasks is devising a logo (8 days), seizing the U.N. (9 days), opening a Starbucks (10 days), training the army (4 days), and then defeating Microsoft (8 days). Since these tasks must be done sequentially, galactic conquest will require at least 39 days.

If there were enough workers, this answer would be correct; however, with only two workers, Liz and Oscar may be unable to make progress on the critical path every day. For example, suppose there were only four tasks: devise logo, build fleet, seize control, get shots. Now the critical path consists of two critical tasks: devise logo, get shots, which take 19 days. But to get through this path in 19 days, some worker must be working on a critical task at all times for the 19 days. This leaves only one worker free to complete building the fleet and seizing control, which will take at least 27 days. So in fact, 27 days is the minimum time for two workers to complete these four tasks. ■

(d) What is the minimum number of days that Liz and Oscar need to conquer the galaxy? No proof is required.

Solution. 40 days. Tasks could be divided as follows:

Oscar: #1 (days 1-8), #3 (days 9-17), #4 (days 18-28), #8 (days 33-40).

Liz: #2 (days 1-18), #5 (days 19-28), #6 (days 29-32), #7 (days 33-38).

It takes some care to verify that 40 days is the best you can do. If someone comes up with a simple proof of this, tell the course staff.

■

Problem 3. (a) What are the maxim*al* and minim*al* elements, if any, of the power set $\mathcal{P}(\{1, \ldots, n\})$, where n is a positive integer, under the *empty relation*?

Solution. The power set is a red herring. With an empty relation on any set, every element is maximal and minimal. ■

(b) What are the maxim*al* and minim*al* elements, if any, of the set, $\mathbb{N}$, of all nonnegative integers under divisibility? Is there a minim*um* or maxim*um* element?

Solution. The minimum (and therefore unique minimal) element is 1 since 1 divides all natural numbers. The maximum (and therefore unique maximal) element is 0 since all numbers divide 0. ■

(c) What are the minimal and maximal elements, if any, of the set of integers greater than 1 under divisibility?

Solution. All prime numbers are minimal elements, since no numbers divide them.

There is no maximal element, because for any $n > 1$, there is a "larger" number under the divisibility partial order, for example, $2n$. ■

(d) Describe a partially ordered set that has no minimal or maximal elements.

Solution. $\mathbb{Z}$, $\mathbb{R}$, etc. ■

(e) Describe a partially ordered set that has a *unique minimal* element, but no minimum element. *Hint:* It will have to be infinite.

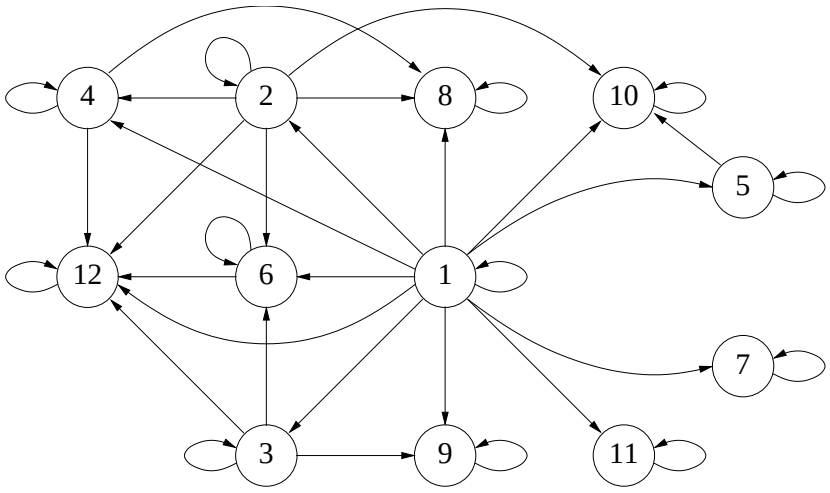
Solution. $\mathbb{Z} \cup \{i\}$ where i is a root of -1, under the usual order $\mathbb{Z}$. So i is incomparable to everything but itself, and is therefore minimal —and maximal too. The remaining elements are the integers, and none of them are minimal since $n - 1 < n$, which makes i unique. ■

6.042J / 18.062J Mathematics for Computer Science
Spring 2010

Solutions to In-Class Problems Week 5, Mon.

Problem 1.
If a and b are distinct nodes of a digraph, then a is said to *cover* b if there is an edge from a to b and every path from a to b traverses this edge. If a covers b, the edge from a to b is called a *covering edge*.

(a) What are the covering edges in the following DAG?



Solution. TBA ■

(b) Let covering (D) be the subgraph of D consisting of only the covering edges. Suppose D is a finite DAG. Explain why covering (D) has the same positive path relation as D.

Hint: Consider *longest* paths between a pair of vertices.

Solution. What we need to show is that if there is a path in D between vertices $a \neq b$, then there is a path consisting only of covering edges from a to b. But since D is a finite DAG, there must be a *longest* path from a to b. Now every edge on this path must be a covering edge or it could be replaced by a path of length 2 or more, yielding a longer path from a to b. ■

(c) Show that if two *DAG*'s have the same positive path relation, then they have the same set of covering edges.

Solution. *Proof.* Suppose C and D are DAG's with the same positive path relation and that $a \to b$ is a covering edge of C. We want to show that $a \to b$ must also be a covering edge of D.

Since $a \to b$ itself defines a (length one) positive length path in C, there must be a positive length path in D from a to b. If this positive length path in D is of length greater than one, then the path must consist of a positive length path from a to c followed by a positive length path from c to b for some vertex, c. Also, since D is a DAG, c cannot be a or b.

This means there must also be positive length paths in C from a to c and from c to b, and neither of these paths can traverse $a \to b$ or there would be a cycle. Hence the path from a to c to b is a path in C that does not traverse $a \to b$, contradicting the fact that $a \to b$ is a covering edge of C.

In sum, there is a length one path from a to b in D, namely $a \to b$, and this is the *only* path from a to b in D, which proves that $a \to b$ is a covering edge in D. ■

(d) Conclude that covering (D) is the *unique* DAG with the smallest number of edges among all digraphs with the same positive path relation as D.

Solution. By part (c), any DAG with the same positive path relation as D must contain all the edges of covering (D). By part (b), covering (D) has this same positive path relation. It follows immediately that covering (D) is the unique minimum-size DAG with the same positive path relation as D. ■

The following examples show that the above results don't work in general for digraphs with cycles.

(e) Describe two graphs with vertices $\{1, 2\}$ which have the same set of covering edges, but not the same positive path relation (*Hint:* Self-loops.)

Solution. Let one graph have edges $\{(1, 2), (1, 1)\}$ and the other $\{(1, 2), (2, 2)\}$. They have the same set of covering edges, namely, $(1, 2)$. But in the second there is a positive length path from 2 to 2, namely a path of length one but there is no positive length path from 2 to 2 in the first graph. ■

(f) (i) The *complete digraph* without self-loops on vertices $1, 2, 3$ has edges between every two distinct vertices. What are its covering edges?

(ii) What are the covering edges of the graph with vertices $1, 2, 3$ and edges $1 \to 2, 2 \to 3, 3 \to 1$?

(iii) What about their positive path relations?

Solution. (i) There are no covering edges, since there is always a length two path from a to b that does not use the edge $a \to b$.

(ii) All three edges are the covering edges.

(iii) They have the same positive path relation, namely, each vertex is connected to all the vertices, including itself, by positive length paths.

■

Problem 2. (a) Give an example showing that two vertices in a digraph may be on the same cycle, but *not* necessarily on the same *simple* cycle.

Solution. Let the vertices be a, b, c and edges be $(a, b), (b, a), (b, c), (c, b)$. Now a and c are on the cyle a, b, c, b, a, but every cycle from a to c must go through b at least twice, and so will not be simple. ■

(b) Prove that if two vertices in a digraph are connected, then they are connected by a simple path. *Hint:* the shortest path.

Solution. Consider a shortest path from a to $b \neq a$:

$$a = a_0, a_1, \ldots, a_i, \ldots, a_j, \ldots, a_k = b,$$

and suppose this path is not simple. That is, suppose $a_i = a_j$ for some i, j. Then

$$a = a_0, a_1, \ldots, a_i, a_{j+1}, \ldots, a_k = b.$$

is a shorter path from a to b, a contradiction.

■

Problem 3.
In an n-player *round-robin tournament*, every pair of distinct players compete in a single game. Assume that every game has a winner —there are no ties. The results of such a tournament can then be represented with a *tournament digraph* where the vertices correspond to players and there is an edge $x \to y$ iff x beat y in their game.

(a) Explain why a tournament digraph cannot have cycles of length 1 or 2.

Solution. There are no self-loops in a tournament graph since no player plays himself, so no length 1 cycles. Also, it cannot be that x beats y and y beats x for $x \neq y$, since every pair competes exactly once and there are no ties. This means there are no length 2 cycles.

■

(b) Is the "beats" relation for a tournament graph always/sometimes/never:

- asymmetric?
- reflexive?
- irreflexive?
- transitive?

Explain.

Solution. No self-loops implies the relation is irreflexive. It is also asymmetric since it is irreflexive and for every pair of distinct players, exactly one game is played and results in a win for one of the players. Some tournament graphs represent transitive relations and others don't. ■

(c) Show that a tournament graph represents a total order iff there are no cycles of length 3.

Solution. As observed in the previous part, the "beats" relation whose graph is a tournament is asymmetric and irreflexive. Since every pair of players is comparable, the relation is a total order iff it is transitive.

"Beats" is transitive iff for any players x, y and z, $x \to y$ and $y \to z$ implies that $x \to z$ (and consequently that there is no edge $z \to x$). Therefore, "beats" is transitive iff there are no cycles of length 3. ■

6.042J / 18.062J Mathematics for Computer Science
Spring 2010

Solutions to In-Class Problems Week 5, Wed.

By now you are very familiar with the 6.042 icon that appears on the course webpage and lecture slides. This icon is a picture of a game called the **Fifteen Puzzle**. The following problem may help you appreciate why this icon was chosen as the course logo.

Problem 1.
In this problem you will establish a basic property of a puzzle toy called the *Fifteen Puzzle* using the method of invariants. The Fifteen Puzzle consists of sliding square tiles numbered $1, \ldots, 15$ held in a 4×4 frame with one empty square. Any tile adjacent to the empty square can slide into it.

The standard initial position is

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

We would like to reach the target position (known in my youth as "the impossible" — ARM):

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

A state machine model of the puzzle has states consisting of a 4×4 matrix with 16 entries consisting of the integers $1, \ldots, 15$ as well as one "empty" entry—like each of the two arrays above.

The state transitions correspond to exchanging the empty square and an adjacent numbered tile. For example, an empty at position $(2, 2)$ can exchange position with tile above it, namely, at position $(1, 2)$:

n_1	n_2	n_3	n_4
n_5		n_6	n_7
n_8	n_9	n_{10}	n_{11}
n_{12}	n_{13}	n_{14}	n_{15}

$\longrightarrow$

n_1		n_3	n_4
n_5	n_2	n_6	n_7
n_8	n_9	n_{10}	n_{11}
n_{12}	n_{13}	n_{14}	n_{15}

We will use the invariant method to prove that there is no way to reach the target state starting from the initial state.

We begin by noting that a state can also be represented as a pair consisting of two things:

1. a list of the numbers $1, \ldots, 15$ in the order in which they appear—reading rows left-to-right from the top row down, ignoring the empty square, and

2. the coordinates of the empty square—where the upper left square has coordinates $(1, 1)$, the lower right $(4, 4)$.

(a) Write out the "list" representation of the start state and the "impossible" state.

Solution. start: $((1\ 2\ \ldots\ 15), (4, 4))$,

impossible: $((15\ 14\ \ldots\ 1), (4, 4))$.

■

Let L be a list of the numbers $1, \ldots, 15$ in some order. A pair of integers is an *out-of-order pair* in L when the first element of the pair both comes *earlier* in the list and *is larger*, than the second element of the pair. For example, the list $1, 2, 4, 5, 3$ has two out-of-order pairs: (4,3) and (5,3). The increasing list $1, 2 \ldots n$ has no out-of-order pairs.

Let a state, S, be a pair $(L, (i, j))$ described above. We define the *parity* of S to be the mod 2 sum of the number, $p(L)$, of out-of-order pairs in L and the row-number of the empty square, that is the parity of S is $p(L) + i \pmod 2$.

(b) Verify that the parity of the start state and the target state are different.

Solution. The parity of the start state is

$$(0 + 4) \bmod 2 = 0.$$

The parity of the target is

$$((15 \cdot 14/2) + 4) \bmod 2 = 1.$$

■

(c) Show that the parity of a state is preserved under transitions. Conclude that "the impossible" is impossible to reach.

Solution. To show that the parity is constant, consider how moves may affect the parity. There are only 4 types of moves: a move to the left, a move to the right, a move to the row above, or a move to the row below.

Note that horizontal moves change nothing, and vertical moves both change i by 1, and move a tile three places forward or back in the list, L. To consider how the parity is changed in this case, we need to consider only the 3 pairs in L that are between the tile's old and new position. (The other pairs are not effected by the tile's move). This reverses the order of three pairs in L, changing the number of inversions by 3 or 1, but always by an odd amount.

To confirm this last remark, note that if the 3 pairs were all out of order or all in order before, the amount is changed by 3. If two pairs were out of order and 1 pair was in order or if one pair was out of order and two were in order, this will change the amount by 1. So the sum of i and the number of out-of-order pairs changes by an even amount (either 1+3 or 1+1), which implies that its parity remains the same. Since the initial state has parity 0 (even), all states reachable from the initial state must have parity 0, so the target state with parity 1 can't be reachable. ■

By the way, if two states have the same parity, then in fact there *is* a way to get from one to the other. If you like puzzles, you'll enjoy working this out on your own.

Problem 2.
The most straightforward way to compute the bth power of a number, a, is to multiply a by itself b times. This of course requires $b-1$ multiplications. There is another way to do it using considerably fewer multiplications. This algorithm is called *fast exponentiation*:

Given inputs $a \in \mathbb{R}, b \in \mathbb{N}$, initialize registers x, y, z to $a, 1, b$ respectively, and repeat the following sequence of steps until termination:

- if $z = 0$ **return** y and terminate
- $r :=$ remainder$(z, 2)$
- $z := \text{quotient}(z, 2)$
- if $r = 1$, then $y := xy$
- $x := x^2$

We claim this algorithm always terminates and leaves $y = a^b$.

(a) Model this algorithm with a state machine, carefully defining the states and transitions.

Solution. 1. The set of states is $\mathbb{R} \times \mathbb{R} \times \mathbb{N}$,

2. The start state is $(a, 1, b)$,
3. the transitions are defined by the rule

$$(x, y, z) \to \begin{cases} (x^2, y, \text{quotient}(z, 2)) & \text{if } z \text{ is positive and even,} \\ (x^2, xy, \text{quotient}(z, 2)) & \text{if } z \text{ is positive and odd.} \end{cases}$$

■

(b) Verify that the predicate $P((x, y, z)) ::= [yx^z = a^b]$ is a preserved invariant.

Solution. We show that P is preserved, namely, assuming $P((x, y, z))$, that is,

$$yx^z = a^b \tag{1}$$

holds and $(x, y, z) \to (x_t, y_t, z_t)$ is a transition, then $P((x_t, y_t, z_t))$, that is,

$$y_t x_t^{z_t} = a^b$$

holds.

We consider two cases:

If $z > 0$ and is even, then we have that $x_t = x^2, y_t = y, z_t = \text{quotient}(z, 2)$. Therefore,

$$\begin{aligned} y_t x_t^{z_t} &= y x^{2 \cdot \text{quotient}(z,2)} \\ &= y x^{2 \cdot (z/2)} \\ &= y x^z \\ &= a^b \qquad \text{(by (1))} \end{aligned}$$

If $z > 0$ and is odd, then we have that $x_t = x^2, y_t = xy, z_t = \text{quotient}(z, 2)$. Therefore,

$$\begin{aligned} y_t x_t^{z_t} &= xy x^{2 \cdot \text{quotient}(z,2)} \\ &= y x^{1+2 \cdot (z-1)/2} \\ &= y x^{1+(z-1)} \\ &= y x^z \\ &= a^b \qquad \text{(by (1))} \end{aligned}$$

So in both cases, $P((x_t, y_t, z_t))$ holds, proving that P is a preserved invariant. ■

(c) Prove that the algorithm is partially correct: if it halts, it does so with $y = a^b$.

Solution. P holds for the start state $(a, 1, b)$ since $1 \cdot a^b = a^b$. So by the Invariant Theorem, P holds for all reachable states. But a terminal state must have $z = 0$, so if any terminal state $(x, y, 0)$ is reachable, then $y = yx^0 = a^b$ as required. ■

(d) Prove that the algorithm terminates.

Solution. Just notice that z is a natural-number-valued variable that gets smaller at every transition. So by the Well-Ordering Principle, when this variable reaches its minimum value, the algorithm terminates. ■

(e) In fact, prove that it requires at most $2 \lceil \log_2(b+1) \rceil$ multiplications for the Fast Exponentiation algorithm to compute a^b for $b > 1$.

Solution. The value of z is initially b and gets at least halved at every step. So it can't be halved more than $\lceil \log_2(b+1) \rceil$ times before hitting zero. We need $(b+1)$ because for $b = 2^p$, a power of two, it takes $(p+1)$ halves to get zero. Since each of the transitions involves at most two multiplications, the total number of multiplications until $z = 0$ is at most $2 \lceil \log_2(b+1) \rceil$. ■

6.042J / 18.062J Mathematics for Computer Science
Spring 2010

Solutions to In-Class Problems Week 5, Fri.

Problem 1.
The Massachusetts Turnpike Authority is concerned about the integrity of the new Zakim bridge. Their consulting architect has warned that the bridge may collapse if more than 1000 cars are on it at the same time. The Authority has also been warned by their traffic consultants that the rate of accidents from cars speeding across bridges has been increasing.

Both to lighten traffic and to discourage speeding, the Authority has decided to make the bridge *one-way* and to put tolls at *both* ends of the bridge (don't laugh, this is Massachusetts). So cars will pay tolls both on entering and exiting the bridge, but the tolls will be different. In particular, a car will pay \$3 to enter onto the bridge and will pay \$2 to exit. To be sure that there are never too many cars on the bridge, the Authority will let a car onto the bridge only if the difference between the amount of money currently at the entry toll booth minus the amount at the exit toll booth is strictly less than a certain threshold amount of $\$T_0$.

The consultants have decided to model this scenario with a state machine whose states are triples of natural numbers, (A, B, C), where

- A is an amount of money at the entry booth,
- B is an amount of money at the exit booth, and
- C is a number of cars on the bridge.

Any state with $C > 1000$ is called a *collapsed* state, which the Authority dearly hopes to avoid. There will be no transition out of a collapsed state.

Since the toll booth collectors may need to start off with some amount of money in order to make change, and there may also be some number of "official" cars already on the bridge when it is opened to the public, the consultants must be ready to analyze the system started at *any* uncollapsed state. So let A_0 be the initial number of dollars at the entrance toll booth, B_0 the initial number of dollars at the exit toll booth, and $C_0 \leq 1000$ the number of official cars on the bridge when it is opened. You should assume that even official cars pay tolls on exiting or entering the bridge after the bridge is opened.

(a) Give a mathematical model of the Authority's system for letting cars on and off the bridge by specifying a transition relation between states of the form (A, B, C) above.

Solution. State (A, B, C) goes to state

(i) $(A + 3, B, C + 1)$, provided that $A - B < T_0$ and $C \leq 1000$. This transition models the case where a car enters the bridge.

(ii) $(A, B+2, C-1)$, provided that $0 < C \leq 1000$. This transition models the case where a car leaves the bridge.

Note that the condition for the first transition has $C \leq 1000$ instead of $C < 1000$. A car can enter so long as it is not in the collapsed state ($C > 1000$). In other words, a car may still enter when $C = 1000$; and the next state will be a collapsed state with $C = 1001 > 1000$.

■

(b) Characterize each of the following derived variables

$$A, B, A+B, A-B, 3C-A, 2A-3B, B+3C, 2A-3B-6C, 2A-2B-3C$$

as one of the following

constant	C
strictly increasing	SI
strictly decreasing	SD
weakly increasing but not constant	WI
weakly decreasing but not constant	WD
none of the above	N

and briefly explain your reasoning.

Solution. In every transition, at least one of A and B increases. So their sum is strictly increasing. $2A - 3B$ can fluctuate, going up on (i) and down on (ii).

The difference $3C - A$ doesn't change under transitions of type (i), but decreases under transitions of type (ii); so is weakly decreasing.

However, $B+3C$ increases under transitions of type (i), but decreases under transitions of type (ii).

On the other hand, $6C$ and $2A - 3B$ simultaneously increase by 6 under transition (i) or simultaneously decrease by 6 under transition (ii), which makes their difference constant.

Finally, under (i), $2A$ increases by 6, B is unchanged, and $3C$ increases by 3, so $2A - 2B - 3C$ increases by $6 - 3 = 3$. However, under (ii), A is unchanged, $3C$ decreases by 3 and $2B$ increases by 4, so $2A - 2B - 3C$ decreases by $-(-4) - 3 = 1$.

The completed table follows.

A	WI
B	WI
$A+B$	SI
$A-B$	N
$3C-A$	WD
$2A-3B$	N
$B+3C$	N
$2A-3B-6C$	C
$2A-2B-3C$	N

■

The Authority has asked their engineering consultants to determine T and to verify that this policy will keep the number of cars from exceeding 1000.

The consultants reason that if C_0 is the number of official cars on the bridge when it is opened, then an additional $1000 - C_0$ cars can be allowed on the bridge. So as long as $A - B$ has not increased by $3(1000 - C_0)$, there shouldn't more than 1000 cars on the bridge. So they recommend defining

$$T_0 ::= 3(1000 - C_0) + (A_0 - B_0), \tag{1}$$

where A_0 is the initial number of dollars at the entrance toll booth, B_0 is the initial number of dollars at the exit toll booth.

(c) Use the results of part (b) to define a simple predicate, P, on states of the transition system which is satisfied by the start state, that is $P(A_0, B_0, C_0)$ holds, is not satisfied by any collapsed state, and is a preserved invariant of the system. Explain why your P has these properties.

Solution. Let $D_0 ::= 2A_0 - 3B_0 - 6C_0$.

Preserved Invariant:

$$P(A, B, C) ::= [2A - 3B - 6C = D_0] \text{ AND } [C \leq 1000].$$

Note that $P(A_0, B_0, C_0)$ is true because we know that $C_0 \leq 1000$, and it is not true in any collapsed state. To verify that P is preserved, suppose state (A, B, C) has a transition to (A', B', C'), and $P(A, B, C)$ is true. We verify that $P(A', B', C')$ is true by considering the two kinds of transitions.

Transition (i) (a car enters the bridge): so

$$6C' = 6(C+1) = 6C + 6 = (2A - 3B - D_0) + 6 = 2(A+3) - 3B - D_0 = 2A' - 3B' - D_0,$$

which implies that

$$2A' - 3B' - 6C' = D_0, \tag{2}$$

as required.

Also, the transition is possible only if $A - B < T_0$. But this implies

$$\begin{aligned}
6C' &= 2A' - 3B' - D_0 && \text{(by (2))}\\
&= 2(A' - B') - B' - D_0\\
&= 2((A+3) - B) - B - D_0 && \text{(since } A' = A+3,\ B' = B\text{)}\\
&= 2(A - B) - B - D_0 + 6\\
&\le 2(A - B) - B_0 - D_0 + 6 && \text{(since } B \text{ is WI)}\\
&\le 2(T_0 - 1) - B_0 - D_0 + 6 && \text{(since } A - B \le T_0 - 1\text{)}\\
&= 2[3(1000 - C_0) + (A_0 - B_0)] - B_0 - D_0 + 4 \text{(by (1))}\\
&= 6000 - 6C_0 + 2A_0 - 3B_0 - D_0 + 4\\
&= 6004,
\end{aligned}$$

and so $C' \le \lfloor 6004/6 \rfloor = 1000$, as required.

Transition (ii) (a car leaves the bridge): so

$$6C' = 6(C-1) = 6C - 6 = 2A - 3B - 6 = 2A - 3(B+2) = 2A' - 3B'.$$

In addition, $C' < C \le 1000$ so $C' \le 1000$. ■

(d) A clever MIT intern working for the Turnpike Authority agrees that the Turnpike's bridge management policy will be *safe*: the bridge will not collapse. But she warns her boss that the policy will lead to *deadlock*— a situation where traffic can't move on the bridge even though the bridge has not collapsed.

Explain more precisely in terms of system transitions what the intern means, and briefly, but clearly, justify her claim.

Solution. The intern means that any long enough sequence of transitions will arrive at a state in which no transition is possible, even though there are no cars on the bridge. This happens because every time a car enters and then exits the bridge the value of $A - B$ increases by 1. So after 3000 cars have crossed the bridge, no further car can enter the bridge because

$$A - B \ge 3000 + A_0 - B_0 \ge 3(1000 - C_0) + (A_0 - B_0) = T_0.$$

After that, cars can only exit the bridge. So after at most 3000+1000 transitions, the system deadlocks with the bridge empty but no cars allowed onto the bridge.

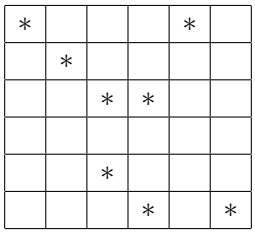
■

Problem 2.

In some terms when 6.042 is not taught in a TEAL room, students sit in a square arrangement during recitations. An outbreak of beaver flu sometimes infects students in recitation; beaver flu

is a rare variant of bird flu that lasts forever, with symptoms including a yearning for more quizzes and the thrill of late night problem set sessions.

Here is an example of a 6×6 recitation arrangement with the locations of infected students marked with an asterisk.

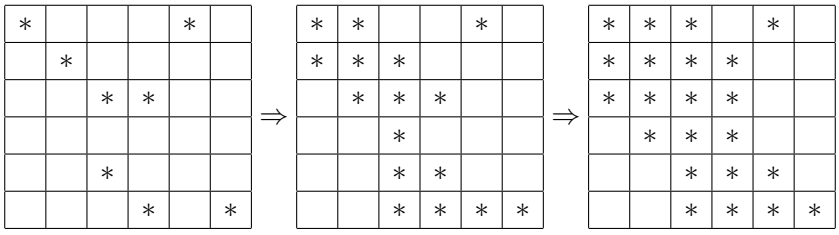


Outbreaks of infection spread rapidly step by step. A student is infected after a step if either

- the student was infected at the previous step (since beaver flu lasts forever), or
- the student was adjacent to *at least two* already-infected students at the previous step.

Here *adjacent* means the students' individual squares share an edge (front, back, left or right, but *not* diagonal). Thus, each student is adjacent to 2, 3 or 4 others.

In the example, the infection spreads as shown below.



In this example, over the next few time-steps, all the students in class become infected.

Theorem. *If fewer than n students among those in an $n \times n$ arrangment are initially infected in a flu outbreak, then there will be at least one student who never gets infected in this outbreak, even if students attend all the lectures.*

Prove this theorem.

Hint: Think of the state of an outbreak as an $n \times n$ square above, with asterisks indicating infection. The rules for the spread of infection then define the transitions of a state machine. Try to derive a weakly decreasing state variable that leads to a proof of this theorem.

Solution. *Proof.* Define the *perimeter* of an infected set of students to be the number of edges with infection on exactly one side. Let ν be size (number of edges) in the perimeter.

We claim that ν is a weakly decreasing variable. This follows because the perimeter changes after a transition only because some squares became newly infected. By the rules above, each newly-infected square is adjacent to at least two previously-infected squares. Thus, for each newly-infected square, at least two edges are removed from the perimeter of the infected region, and at

most two edges are added to the perimeter. Therefore, the perimeter of the infected region cannot increase.

Now if an $n \times n$ grid is completely infected, then the perimeter of the infected region is $4n$. Thus, the whole grid can become infected only if the perimeter is initially at least $4n$. Since each square has perimeter 4, at least n squares must be infected initially for the whole grid to become infected. ■

Problem 3.
Start with 102 coins on a table, 98 showing heads and 4 showing tails. There are two ways to change the coins:

(i) flip over any ten coins, or

(ii) let n be the number of heads showing. Place $n + 1$ additional coins, all showing tails, on the table.

For example, you might begin by flipping nine heads and one tail, yielding 90 heads and 12 tails, then add 91 tails, yielding 90 heads and 103 tails.

(a) Model this situation as a state machine, carefully defining the set of states, the start state, and the possible state transitions.

Solution. This can be modeled by a state machine. The state of the machine is the number of heads and tails. The start state is $(98, 4)$, and the transitions are:

$$(h,t) \to \begin{cases} (h-a+(10-a), t+a-(10-a)) & \text{for } 10 \le h+t \& 0 \le a \le \min(10,h). \\ (h, t+h+1). \end{cases}$$

■

(b) Explain how to reach a state with exactly one tail showing.

Solution. One way is to:

1. Do operation 2 three times, yielding $(98, 4 + 3 \cdot 99) = (98, 301)$.
2. Repeat 30 times: Do operation 1 to flip 10 tails into heads. This will result in the state $(398, 1)$, which is the desired state.

■

(c) Define the following derived variables:

C	::=	the number of coins on the table,	H	::=	the number of heads,
T	::=	the number of tails,	C_2	::=	$\text{remainder}(C/2)$,
H_2	::=	$\text{remainder}(H/2)$,	T_2	::=	$\text{remainder}(T/2)$.

Which of these variables is

1. strictly increasing

   Solution. NONE ■

2. weakly increasing

   Solution. C, H_2 ■

3. strictly decreasing

   Solution. NONE ■

4. weakly decreasing

   Solution. H_2 ■

5. constant

   Solution. H_2 ■

(d) Prove that it is not possible to reach a state in which there is exactly one head showing.

Solution. We claimed above that H_2 is an invariant value, that is, it does not change under state transitions. To prove this, let (h, t) be a state with h even. For the next state, we have two cases to consider:

1. The first operation is executed: $(h, t) \to (h - 2a + 10, t + 2a - 10)$. Since $-2a + 10$ is even, $H_2((h, t)) = H_2(h - 2a + 10, t + 2a - 10)$.
2. The second operation is executed: $(h, t) \to (h, t + h + 1)$. The number of heads does not change in this case, so H_2 does not change.

Since the initial number of heads, 98, is even, that is, $H_2((98, 4)) = 0$, the Invariant Method now implies that the number of heads in a reachable state is always even. But since one is odd, it is not possible to reach a state in which there is exactly one head showing.

■

6.042J / 18.062J Mathematics for Computer Science
Spring 2010

Solutions to In-Class Problems Week 6, Mon.

Problem 1.
Four Students want separate assignments to four VI-A Companies. Here are their preference rankings:

Student	Companies
Albert:	HP, Bellcore, AT&T, Draper
Rich:	AT&T, Bellcore, Draper, HP
Megumi:	HP, Draper, AT&T, Bellcore
Justin:	Draper, AT&T, Bellcore, HP

Company	Students
AT&T:	Justin, Albert, Megumi, Rich
Bellcore:	Megumi, Rich, Albert, Justin
HP:	Justin, Megumi, Albert, Rich
Draper:	Rich, Justin, Megumi, Albert

(a) Use the Mating Ritual to find *two* stable assignments of Students to Companies.

Solution. Treat Students as Boys and the result is the following assignment:

Student	Companies	Rank in the original list
Albert:	Bellcore	2
Rich:	AT&T	1
Megumi:	HP	1
Justin:	Draper	1

Treat Companies as Boys and the result is the following assignment:

Company	Students	Rank in the original list
AT&T:	Albert	2
Bellcore:	Rich	2
HP:	Megumi	2
Draper:	Justin	2

■

(b) Describe a simple procedure to determine whether any given stable marriage problem has a unique solution, that is, only one possible stable matching.

Solution. See if the Mating Ritual with Boys as suitors yields the same solution as the algorithm with Girls as suitors. These two marriage assignments are boy-optimal and boy-pessimal, respective. Obviously, if every boy's optimal and pessimal choices are the same, then every boy has an unique choice. The solution is unique.

■

Problem 2.
A preserved invariant of the Mating ritual is:

> For every girl, G, and every boy, B, if G is crossed off B's list, then G has a favorite suitor and she prefers him over B.

Use the invariant to prove that the Mating Algorithm produces stable marriages. (Don't look up the proof in the Notes or slides.)

Solution. *Proof.* Let Brad be some boy and Jen be any girl that he is *not* married to on the last day of the Mating Ritual. We claim that Brad and Jen are not a rogue couple. Since Brad is an arbitrary boy, it follows that no boy is part of a rogue couple. Hence the marriages on the last day are stable.

To prove the claim, we consider two cases:

Case 1. Jen is not on Brad's list. Then by invariant P, we know that Jen prefers her husband to Brad. So she's not going to run off with Brad: the claim holds in this case.

Case 2. Otherwise, Jen is on Brad's list. But since Brad is not married to Jen, he must be choosing to serenade his wife instead of Jen, so he must prefer his wife. So he's not going to run off with Jen: the claim also holds in this case. ■

Problem 3.
Suppose that Harry is one of the boys and Alice is one of the girls in the *Mating Ritual*. Which of the properties below are preserved invariants? Why?

a. Alice is the only girl on Harry's list.

b. There is a girl who does not have any boys serenading her.

c. If Alice is not on Harry's list, then Alice has a suitor that she prefers to Harry.

d. Alice is crossed off Harry's list and Harry prefers Alice to anyone he is serenading.

e. If Alice is on Harry's list, then she prefers to Harry to any suitor she has.

Solution. The 1st, 3rd, and 4th are preserved invariants.

a. A preserved invariant; no girl will be added to Harry's list. If Alice got crossed off, there would be no one for Harry to marry. So she must remain as the sole girl on his list. **Reminder**: A *preserved invariant* need not be true all the time, as in this example. It only needs to stay true once it first becomes true.

b. Not preserved; a girl may not have a suitor on the first day, —if, for example, she's not at the top of any boy's list —but every girl is guaranteed to have one at the end, namely, her husband.

c. A preserved invariant; this is the basic invariant used to verify the Ritual.

d. A preserved invariant; Harry crosses off the girls in his order of preference, so if Alice is crossed off, Harry likes her better than anybody that's left.

e. Not preserved. Suppose the preferences among two couples and a third boy are:

Harry:	Alice,	Elvira,	...
Billy:	Elvira,	Alice,	...
Wilfred:	Elvira,	...	
Alice:	Billy,	Harry,	...
Elvira:	Wilfred,	Billy,	...

The alleged invariant is true on the first day since Harry is Alice's only suitor. But Elvira rejects Billy in favor of Wilfred on the first afternoon, so on the second day, Billy and Harry are serenading Alice. Since Alice prefers Billy to Harry, the alleged invariant is no longer true, so it was not preserved.

■

Problem 4.
Consider a stable marriage problem with 4 boys and 4 girls and the following partial information about their preferences:

B1:	G1	G2	–	–
B2:	G2	G1	–	–
B3:	–	–	G4	G3
B4:	–	–	G3	G4
G1:	B2	B1	–	–
G2:	B1	B2	–	–
G3:	–	–	B3	B4
G4:	–	–	B4	B3

(a) Verify that

$$(B1, G1), (B2, G2), (B3, G3), (B4, G4)$$

will be a stable matching whatever the unspecified preferences may be.

Solution.
- $B1$ and $B2$ get their 1st choice, so won't be in a rogue couple.
- $G1$ and $G2$ get their 2nd choices, so won't be in a rogue couple with the other two boys, $B3$ or $B4$. So $G1$ and $G2$ won't be in any rogue couple, either.
- $G3$ and $G4$ get their best remaining choices, so will never be in a rogue couple.

- This leaves no possible rogue partners for $B3$ and $B4$.

So the marriages are sure to be stable.

■

(b) Explain why the stable matching above is neither boy-optimal nor boy-pessimal and so will not be an outcome of the Mating Ritual.

Solution. Notice that giving $G1$ and $G2$ their first choices, that is, marrying $(B1, G2)$ and $(B2, G1)$ would also be stable for the same reason. But with this switch, $B1$ does worse. So the stable matching above is not boy-pessimal.

Likewise, after marrying off the first two boys and girls, giving $B3$ and $B4$ their best remaining choices, that is, marrying $(B3, G4), (B4, G3)$, will also be stable. But with this switch, $B3$ does better. So the stable matching above is not boy-optimal.

This implies that the stable matching above would not be produced by the Mating Ritual.

■

(c) Describe how to define a set of marriage preferences among n boys and n girls which have at least $2^{n/2}$ stable assignments.

Hint: Arrange the boys into a list of $n/2$ pairs, and likewise arrange the girls into a list of $n/2$ pairs of girls. Choose preferences so that the kth pair of boys ranks the kth pair of girls just below the previous pairs of girls, and likewise for the kth pair of girls. Within the kth pairs, make sure each boy's first choice girl in the pair prefers the other boy in the pair.

Solution. Suppose a match has the two boys in the kth pair married to the two girls in the kth pair, for $1 \leq k \leq n/2$. A boy John, in the kth pair of boys will never be in a rogue couple with a girl, Jill, who is in the jth pair of girls for $j \neq k$, because if $j > k$, then Jill prefers her partner in the jth pair to John, and if $j < k$ then John prefers his partner in the kth pair to Jill.

A rogue couple can only involve a boy, John, and a girl, Mary, in the same pair, but this is impossible since (exactly) one of John and Mary must be married to their preferred choice in their pair.

Since each boy can be stably married to either of the girls in the kth pair, and there are $n/2$ pairs, the total number of such stable matchings is $2^{n/2}$. ■

6.042J / 18.062J Mathematics for Computer Science
Spring 2010

Solutions to In-Class Problems Week 6, Wed.

Problem 1.
For each of the following pairs of graphs, either define an isomorphism between them, or prove that there is none. (We write ab as shorthand for a—b.)

(a)

$$G_1 \text{ with } V_1 = \{1,2,3,4,5,6\},\ E_1 = \{12,23,34,14,15,35,45\}$$
$$G_2 \text{ with } V_2 = \{1,2,3,4,5,6\},\ E_2 = \{12,23,34,45,51,24,25\}$$

Solution. Not isomorphic: G_2 has a node, 2, of degree 4, but the maximum degree in G_1 is 3. ■

(b)

$$G_3 \text{ with } V_3 = \{1,2,3,4,5,6\},\ E_3 = \{12,23,34,14,45,56,26\}$$
$$G_4 \text{ with } V_4 = \{a,b,c,d,e,f\},\ E_4 = \{ab,bc,cd,de,ae,ef,cf\}$$

Solution. Isomorphic (two isomorphisms) with the vertex correspondences:
$1f, 2c, 3d, 4e, 5a, 6b$
or $1f, 2e, 3d, 4c, 5b, 6a$

■

(c)

$$G_5 \text{ with } V_5 = \{a,b,c,d,e,f,g,h\},\ E_5 = \{ab,bc,cd,ad,ef,fg,gh,he,dh,bf\}$$
$$G_6 \text{ with } V_6 = \{s,t,u,v,w,x,y,z\},\ E_6 = \{st,tu,uv,sv,wx,xy,yz,wz,sw,vz\}$$

Solution. Not isomorphic: they have the same number of vertices, edges, and set of vertex degrees. But the degree 2 vertices of G_1 are all adjacent to two degree 3 vertices, while the degree 2 vertices of G_2 are all adjacent to one degree 2 vertex and one degree 3 vertex.

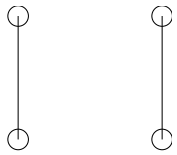
■

Problem 2.
Definition **??**. A graph is *connected* iff there is a path between every pair of its vertices.

False Claim. *If every vertex in a graph has positive degree, then the graph is connected.*

(a) Prove that this Claim is indeed false by providing a counterexample.

Solution. There are many counterexamples; here is one:



■

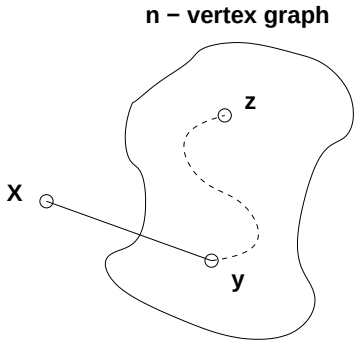
(b) Since the Claim is false, there must be an logical mistake in the following bogus proof. Pinpoint the *first* logical mistake (unjustified step) in the proof.

Bogus proof. We prove the Claim above by induction. Let $P(n)$ be the proposition that if every vertex in an n-vertex graph has positive degree, then the graph is connected.

Base cases: ($n \leq 2$). In a graph with 1 vertex, that vertex cannot have positive degree, so $P(1)$ holds vacuously.

$P(2)$ holds because there is only one graph with two vertices of positive degree, namely, the graph with an edge between the vertices, and this graph is connected.

Inductive step: We must show that $P(n)$ implies $P(n+1)$ for all $n \geq 2$. Consider an n-vertex graph in which every vertex has positive degree. By the assumption $P(n)$, this graph is connected; that is, there is a path between every pair of vertices. Now we add one more vertex x to obtain an $(n+1)$-vertex graph:



All that remains is to check that there is a path from x to every other vertex z. Since x has positive degree, there is an edge from x to some other vertex, y. Thus, we can obtain a path from x to z by going from x to y and then following the path from y to z. This proves $P(n+1)$.

By the principle of induction, $P(n)$ is true for all $n \geq 0$, which proves the Claim.

■

Solution. This one is tricky: the proof is actually a good proof of something else. The first error in the proof is only in the final statement of the inductive step: "This proves $P(n+1)$".

The issue is that to prove $P(n+1)$, *every* $(n+1)$-vertex positive-degree graph must be shown to be connected. But the proof doesn't show this. Instead, it shows that every $(n+1)$-vertex positive-degree graph *that can be built up by adding a vertex of positive degree to an n-vertex connected graph*, is connected.

The problem is that *not every* $(n+1)$-vertex positive-degree graph can be built up in this way. The counterexample above illustrates this: there is no way to build that 4-vertex positive-degree graph from a 3-vertex positive-degree graph.

More generally, this is an example of "buildup error". This error arises from a faulty assumption that every size $n+1$ graph with some property can be "built up" in some particular way from a size n graph with the same property. (This assumption is correct for some properties, but incorrect for others— such as the one in the argument above.)

One way to avoid an accidental build-up error is to use a "shrink down, grow back" process in the inductive step: start with a size $n+1$ graph, remove a vertex (or edge), apply the inductive hypothesis $P(n)$ to the smaller graph, and then add back the vertex (or edge) and argue that $P(n+1)$ holds. Let's see what would have happened if we'd tried to prove the claim above by this method:

Inductive step: We must show that $P(n)$ implies $P(n+1)$ for all $n \geq 1$. Consider an $(n+1)$-vertex graph G in which every vertex has degree at least 1. Remove an arbitrary vertex v, leaving an n-vertex graph G' in which every vertex has degree... uh-oh!

The reduced graph G' might contain a vertex of degree 0, making the inductive hypothesis $P(n)$ inapplicable! We are stuck— and properly so, since the claim is false! ■

Problem 3. (a) Prove that in every graph, there are an even number of vertices of odd degree.

Hint: The Handshaking Lemma **??**.

Solution. *Proof.* Partitioning the vertices into those of even degree and those of odd degree, we know

$$\sum_{v \in V} d(v) \;=\; \sum_{d(v) \text{ is even}} d(v) \;+\; \sum_{d(v) \text{ is odd}} d(v)$$

By the Handshaking Lemma, the value of the lefthand side of this equation equals twice the number of edges, and so is even. The first summand on the righthand side is even since it is a sum of even values. So the second summand on the righthand side must also be even. But since it is entirely a sum of odd values, it must must contain an even number of terms. That is, there must be an even number of vertices with odd degree. ■

(b) Conclude that at a party where some people shake hands, the number of people who shake hands an odd number of times is an even number.

Solution. We can represent the people at the party by the vertices of a graph. If two people shake hands, then there is an edge between the corresponding vertices. So the degree of a vertex is the number of handshakes the corresponding person performed. The result in the first part of this problem now implies that there are an even number of odd-degree vertices, which translates into an even number of people who shook an odd number of hands. ■

(c) Call a sequence of two or more different people at the party a *handshake sequence* if, except for the last person, each person in the sequence has shaken hands with the next person in the sequence.

Suppose George was at the party and has shaken hands with an odd number of people. Explain why, starting with George, there must be a handshake sequence ending with a different person who has shaken an odd number of hands.

Hint: Just look at the people at the ends of handshake sequences that start with George.

Solution. The handshake graph between just the people at the ends of handshake sequences that start with George is a graph, so by part (b), it must have an even number of people who shake an odd number of hands. In particular, there must be at least one other person besides George, call him Harry, who has also shaken an odd number of hands. So the handshake sequence from George that ends with Harry is what we were looking for. ■

6.042J / 18.062J Mathematics for Computer Science
Spring 2010

Solutions to In-Class Problems Week 6, Fri.

Problem 1.
Prove that a graph is a tree iff it has a unique simple path between any two vertices.

Solution. Theorem 10.3.1 shows that in a tree there are unique simple paths between any two vertices.

Conversely, suppose we have a graph, G, with unique paths. Now G is connected since there is a path between any two vertices. So we need only show that G has no simple cycles. But if there was a simple cycle in G, there are two paths between any two vertices on the cycle (going one way around the cycle or the other way around), a violation of uniqueness. So G must cannot have any simple cycles. ■

Problem 2.
The n-dimensional hypercube, H_n, is a graph whose vertices are the binary strings of length n. Two vertices are adjacent if and only if they differ in exactly 1 bit. For example, in H_3, vertices `111` and `011` are adjacent because they differ only in the first bit, while vertices `101` and `011` are not adjacent because they differ at both the first and second bits.

(a) Prove that it is impossible to find two spanning trees of H_3 that do not share some edge.

Solution. H_3 has 8 vertices so every spanning tree has 7 edges. But H_3 has only 12 edges, so any two sets of 7 edges must overlap.

■

(b) Verify that for any two vertices $x \neq y$ of H_3, there are 3 paths from x to y in H_3, such that, besides x and y, no two of those paths have a vertex in common.

Solution. Define the distance between two binary strings of length n to be the number of positions at which they differ (this is known as the *Hamming distance* between the strings).

To show that there are 3 paths between any two distance 1 strings, we can, by symmetry, just consider paths between the vertices `000` and `001`.

Paths from `000` to `001`:

$$\begin{aligned} &000, 001\\ &000, 010, 011, 001\\ &000, 100, 101, 001 \end{aligned}$$

Likewise for distance 2, it is enough to find paths between 000 and 011:

$$\begin{aligned} &000, 010, 011\\ &000, 001, 011\\ &000, 100, 110, 111, 011 \end{aligned}$$

Finally, for distance 3 from 000 to 111:

$$\begin{aligned} &000, 001, 011, 111\\ &000, 010, 110, 111\\ &000, 100, 101, 111 \end{aligned}$$

■

(c) Conclude that the connectivity of H_3 is 3.

Solution. Since there are three paths from x to y in H_3 that share no edges with one another, removing any two edges will leave one of these paths intact, so x and y remain connected. So removing two edges from H_3 does not disconnect it.

On the other hand, removing all 3 edges incident to any vertex, disconnects that vertex. Thus the minimum number of edges necessary to disconnect H_3 is 3. ■

(d) Try extending your reasoning to H_4. (In fact, the connectivity of H_n is n for all $n \geq 1$. A proof appears in the problem solution.)

Solution. Two paths in a graph are said to *cross* when they have a vertex in common other than their endpoints. A set of paths in a graph *don't cross* when no two paths in the set cross. A graph is *k-routed* if between every pair of distinct vertices in the graph there is a set of k paths that don't cross.

We'll show that

Lemma 2.1.

$$H_n \text{ is } n\text{-routed for all } n \geq 1.$$

Since H_n can be disconnected by deleting the n edges incident to any vertex, this implies that H_n has connectivity n.

Proof. The proof is by induction on n with induction hypothesis,

$$P(n) ::= H_n \text{ is } n\text{-routed}.$$

Base case [$n = 1$]: Since H_1 consists of two vertices connected by an edge, $P(1)$ is immediate.

Base case [$n = 2$]: H_2 is a square. Vertices on opposite corners are obviously connected by two length 2 paths that don't cross, and adjacent vertices are connected by a length 1 path and a length 3 path.

Inductive step: We prove $P(n+1)$ for $n \geq 2$ by letting v and w be two vertices of H_{n+1} and describing $n+1$ paths between them that don't cross.

Let R by any positive length path in H_n, say

$$R = r_0, r_1, \ldots, r_k.$$

For $b \in \{0, 1\}$ define the H_{n+1} path

$$bR ::= br_0, br_1, \ldots, br_k.$$

Case 1: The distance from v to w is $d \leq n$. In this case, the $(n+1)$-bit strings v and w agree in one or more positions. By symmetry, we can assume without loss of generality that v and w both start with 0. That is $v = 0v'$ and $w = 0w'$ for some n-bit strings v', w'. Now by induction, there are paths, Q_i for $1 \leq i \leq n$, that don't cross going between v' and w' in H_n.

Define the first n paths in H_{n+1} between v and w to be

$$\pi_i ::= 0Q_i$$

for $1 \leq i \leq n$. These paths don't cross since the Q_i's don't cross.

Then define the $n+1$st path

$$\pi_{n+1} ::= v,\ 1\pi_{v',w'},\ w$$

where $\pi_{v',w'}$ is any simple path from v' to w' in H_n. Then π_{n+1} obviously does not cross any of the other paths since $1\pi_{v',w'}$ is vertex disjoint from $0Q_i$ for $1 \leq i \leq n$.

This proves that $P(n+1)$ hold in this case.

Case 2: The distance from v to w is $n+1$. By symmetry, we can assume without loss of generality that $v = 0^{n+1}$ and $w = 1^{n+1}$.

Now by induction, there are n paths from 0^n to 1^n in H_n that don't cross in H_n. We can assume wlog[1] that each of these paths is simple.

Removing the shared first vertex, 0^n, of these paths yields paths $R_1, R_2, \ldots, R_n$. Now the R_i's are vertex disjoint except for their common endpoint, 1^n. Let s_i be the start vertex of the R_i for $1 \leq i \leq n$.

We now define $n+1$ paths in H_{n+1} from 0^{n+1} to 1^{n+1} that don't cross.

The first of these paths will be

$$\pi_1 ::= 0^{n+1}, 10^n, 1R_1.$$

For $2 \leq i \leq n$, the ith of these paths will be

$$\pi_i ::= 0^{n+1}, 0s_i, 1R_i.$$

These paths don't cross because

- the paths $1R_i$ for $1 \leq i \leq n$ are vertex disjoint except for their common endpoint, 1^{n+1}, because the R_i's are vertex disjoint except for their common endpoint, 1^n,

[1] *without loss of generality*

- a vertex $0s_i$ does not appear on π_j for any for $j \neq i$ because the $s_i \neq s_j$ for $j \neq i$, and the other vertices on the π_j's start with 1,
- the vertex 10^n appears only on π_1. This follows because if it appeared on π_i for $i \neq 1$ it must appear on $1R_i$. That would imply that 0^n appears on R_i, contradicting the fact that the original path $0^n, R_i$ in H_n is simple.

Finally, the $n+1$st path will be

$$\pi_{n+1} ::= 0^{n+1}, 0R_1, 1^{n+1}.$$

Note that, since all but the final vertex on π_{n+1} start with 0, the only vertices besides the endpoints that π_{n+1} could share with another path would be $0s_i$ for $2 \leq i \leq n$. But none of these appear on π_{n+1} because, except for their shared endpoint, R_1 is vertex disjoint from all the other R_i's.

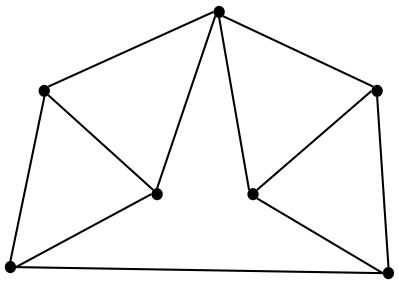
This proves that $P(n+1)$ holds in case 2, and therefore holds in all cases, which completes the proof by induction. ■

Note that this proof implicitly defines a recursive procedure that, for any two vertices in H_n, finds between the two vertices n simple paths of length at most $n+1$ that don't cross. ■

6.042J / 18.062J Mathematics for Computer Science
Spring 2010

Solutions to In-Class Problems Week 7, Mon.

Problem 1.
Let G be the graph below[1]. Carefully explain why $\chi(G) = 4$.



Solution. Four colors are sufficient, so $\chi(G) \leq 4$.

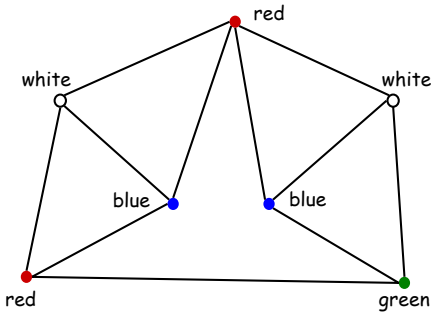


Figure 1: A 4-coloring of the Graph

Now assume $\chi(G) = 3$. We may assume the top vertex is colored red. The top two triangles require 3 colors each, and since they share the top red vertex, they must have the other two colors, white and blue, at their bases, as in Figure 1. Now the bottom two vertices are both adjacent to vertices colored white and blue, and cannot have the same color since they are adjacent, so there is no alternative but to color one with a third color and the other with a fourth color, contradicting the assumption that 3 colors are enough. Hence, $\chi(G) > 3$. This together with the coloring of Figure 1 implies that $\chi(G) = 4$. ■

[1] From *Discrete Mathematics*, Lovász, Pelikan, and Vesztergombi. Springer, 2003. Exercise 13.3.1

Problem 2.
A portion of a computer program consists of a sequence of calculations where the results are stored in variables, like this:

	Inputs:		a, b
Step 1.	c	$=$	$a + b$
2.	d	$=$	$a * c$
3.	e	$=$	$c + 3$
4.	f	$=$	$c - e$
5.	g	$=$	$a + f$
6.	h	$=$	$f + 1$
	Outputs:		d, g, h

A computer can perform such calculations most quickly if the value of each variable is stored in a *register*, a chunk of very fast memory inside the microprocessor. Programming language compilers face the problem of assigning each variable in a program to a register. Computers usually have few registers, however, so they must be used wisely and reused often. This is called the *register allocation* problem.

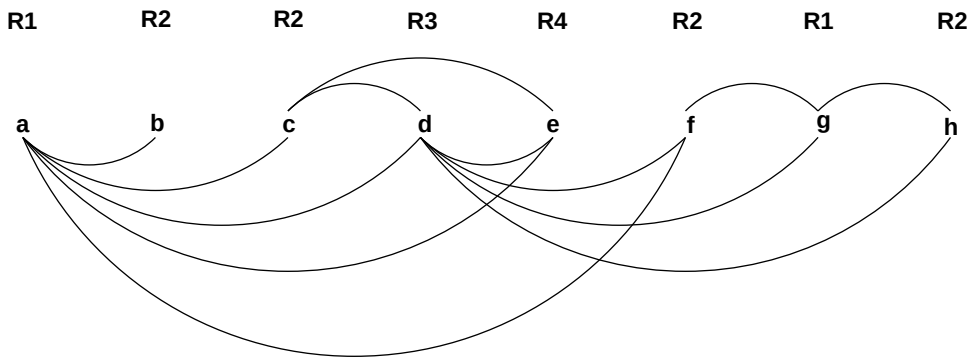
In the example above, variables a and b must be assigned different registers, because they hold distinct input values. Furthermore, c and d must be assigned different registers; if they used the same one, then the value of c would be overwritten in the second step and we'd get the wrong answer in the third step. On the other hand, variables b and d may use the same register; after the first step, we no longer need b and can overwrite the register that holds its value. Also, f and h may use the same register; once $f + 1$ is evaluated in the last step, the register holding the value of f can be overwritten.(Assume that the computer carries out each step in the order listed and that each step is completed before the next is begun.)

(a) Recast the register allocation problem as a question about graph coloring. What do the vertices correspond to? Under what conditions should there be an edge between two vertices? Construct the graph corresponding to the example above.

Solution. There is one vertex for each variable. An edge between two vertices indicates that the values of the variables must be stored in different registers.

We can classify each appearance of a variable in the program as either an *assignment* or a *use*. In particular, an appearance is an assignment if the variable is on the left side of an equation or on the "Inputs" line. An appearance of a variable is a use if the variable is on the right side of an equation or on the "Outputs" line. The *lifetime of a variable* is the segment of code extending from the initial assignment of the variable until the last use.[2] There is an edge between two variables if their lifetimes overlap. This rule generates the following graph:

[2]This definition is for the case that each variable is assigned at most once (see part (c)).



■

(b) Color your graph using as few colors as you can. Call the computer's registers $R1$, $R2$, etc. Describe the assignment of variables to registers implied by your coloring. How many registers do you need?

Solution. Four registers are needed.

One possible assignment of variables to registers is indicated in the figure above. In general, coloring a graph using the minimum number of colors is quite difficult; no efficient procedure is known. However, the register allocation problem always leads to an *interval graph*, and optimal colorings for interval graphs are always easy to find. This makes it easy for compilers to allocate a minimum number of registers. ■

(c) Suppose that a variable is assigned a value more than once, as in the code snippet below:

$$\begin{aligned} &\ldots \\ t &= r + s \\ u &= t * 3 \\ t &= m - k \\ v &= t + u \\ &\ldots \end{aligned}$$

How might you cope with this complication?

Solution. Each time a variable is reassigned, we could regard it as a completely new variable. Then we would regard the example as equivalent to the following:

$$\begin{aligned} &\ldots \\ t &= r + s \\ u &= t * 3 \\ t' &= m - k \\ v &= t' + u \\ &\ldots \end{aligned}$$

We can now proceed with graph construction and coloring as before. ■

Problem 3.
MIT has a lot of student clubs loosely overseen by the MIT Student Association. Each eligible club would like to delegate one of its members to appeal to the Dean for funding, but the Dean will not allow a student to be the delegate of more than one club. Fortunately, the Association VP took 6.042 and recognizes a matching problem when she sees one.

(a) Explain how to model the delegate selection problem as a bipartite matching problem.

Solution. Define a bipartite graph with the student clubs as one set of vertices and everybody who belongs to some club as the other set of vertices. Let a club and a student be adjacent exactly when the student belongs to the club. Now a matching of clubs to students will give a proper selection of delegates: every club will have a delegate, and every delegate will represent exactly one club. ■

(b) The VP's records show that no student is a member of more than 9 clubs. The VP also knows that to be eligible for support from the Dean's office, a club must have at least 13 members. That's enough for her to guarantee there is a proper delegate selection. Explain. (If only the VP had taken 6.046, *Algorithms*, she could even have found a delegate selection without much effort.)

Solution. The degree of every club is at least 13, and the degree of every student is at most 9, so the graph is *degree-constrained* (see the Appendix) which implies there will be no bottlenecks to prevent a matching. Hall's Theorem then guarantees a matching. ■

Problem 4.
A *Latin square* is $n \times n$ array whose entries are the number $1, \ldots, n$. These entries satisfy two constraints: every row contains all n integers in some order, and also every column contains all n integers in some order. Latin squares come up frequently in the design of scientific experiments for reasons illustrated by a little story in a footnote[3]

[3] At Guinness brewery in the eary 1900's, W. S. Gosset (a chemist) and E. S. Beavan (a "maltster") were trying to improve the barley used to make the brew. The brewery used different varieties of barley according to price and availability, and their agricultural consultants suggested a different fertilizer mix and best planting month for each variety.

Somewhat sceptical about paying high prices for customized fertilizer, Gosset and Beavan planned a season long test of the influence of fertilizer and planting month on barley yields. For as many months as there were varieties of barley, they would plant one sample of each variety using a different one of the fertilizers. So every month, they would have all the barley varieties planted and all the fertilizers used, which would give them a way to judge the overall quality of that planting month. But they also wanted to judge the fertilizers, so they wanted each fertilizer to be used on each variety during the course of the season. Now they had a little mathematical problem, which we can abstract as follows.

Suppose there are n barley varieties and an equal number of recommended fertilizers. Form an $n \times n$ array with a column for each fertilizer and a row for each planting month. We want to fill in the entries of this array with the integers 1,...,n numbering the barley varieties, so that every row contains all n integers in some order (so every month each variety is planted and each fertilizer is used), and also every column contains all n integers (so each fertilizer is used on all the varieties over the course of the growing season).

For example, here is a 4×4 Latin square:

1	2	3	4
3	4	2	1
2	1	4	3
4	3	1	2

(a) Here are three rows of what could be part of a 5×5 Latin square:

2	4	5	3	1
4	1	3	2	5
3	2	1	5	4

Fill in the last two rows to extend this "Latin rectangle" to a complete Latin square.

Solution. Here is one possible solution:

2	4	5	3	1
4	1	3	2	5
3	2	1	5	4
1	5	2	4	3
5	3	4	1	2

■

(b) Show that filling in the next row of an $n \times n$ Latin rectangle is equivalent to finding a matching in some $2n$-vertex bipartite graph.

Solution. Construct a bipartite graph as follows. One set of vertices are the columns of the Latin rectangle, and the other set is the numbers 1 to n. Put an edge between a column and a number if the number has *not yet appeared* in the column. Thus, a matching in this graph would associate each column with a distinct number that has not yet appeared in that column. These numbers would form the next row of the Latin rectangle. ■

(c) Prove that a matching must exist in this bipartite graph and, consequently, a Latin rectangle can always be extended to a Latin square.

Solution. Suppose the Latin rectangle has k rows of width n. Then each column-vertex has degree $n-k$ because its edges go to the $n-k$ numbers missing from the column. Also, each number-vertex

also has degree $n - k$. That's because each number appears exactly once in each of the k rows and at most once in each column, so each number must be missing from exactly $n - k$ columns.

So the graph is degree-constrained and therefore has a matching. This implies that we can add rows to the Latin rectangle by the procedure described above as long as $k < n$. At that point, we have a Latin square. ■

6.042J / 18.062J Mathematics for Computer Science
Spring 2010

Solutions to In-Class Problems Week 7, Wed.

Problem 1.
The Elementary 18.01 Functions (F18's) are the set of functions of one real variable defined recursively as follows:

Base cases:

- The identity function, $\mathrm{id}(x) ::= x$ is an F18,
- any constant function is an F18,
- the sine function is an F18,

Constructor cases:

If f, g are F18's, then so are

1. $f + g$, fg, e^g (the constant e),
2. the inverse function $f^{(-1)}$,
3. the composition $f \circ g$.

(a) Prove that the function $1/x$ is an F18.

Warning: Don't confuse $1/x = x^{-1}$ with the inverse, $\mathrm{id}^{(-1)}$ of the identity function $\mathrm{id}(x)$. The inverse $\mathrm{id}^{(-1)}$ is equal to id.

Solution. $\log x$ is the inverse of e^x so $\log x \in$ F18. Therefore so is $c \cdot \log x$ for any constant c, and hence $e^{c \log x} = x^c \in$ F18. Now let $c = -1$ to get $x^{-1} = 1/x \in$ F18.[1] ■

(b) Prove by Structural Induction on this definition that the Elementary 18.01 Functions are *closed under taking derivatives*. That is, show that if $f(x)$ is an F18, then so is $f' ::= df/dx$. (Just work out 2 or 3 of the most interesting constructor cases; you may skip the less interesting ones.)

Solution. *Proof.* By Structural Induction on def of $f \in$ F18. The induction hypothesis is the above statement to be shown.

[1] There's a little problem here: since $\log x$ is not real-valued for $x \leq 0$, the function $f(x) ::= 1/x$ constructed in this way is only defined for $x > 0$. To get an F18 equal to $1/x$ defined for all $x \neq 0$, use $(x/|x|) \cdot f(|x|)$, where $|x| = \sqrt{x^2}$.

Base Cases: We want to show that the derivatives of all the base case functions are in F18.

This is easy: for example, $d\,\mathrm{id}(x)/dx = 1$ is a constant function, and so is in F18. Similarly, $d\sin(x)/dx = \cos(x)$ which is also in F18 since $\cos(x) = \sin(x + \pi/2) \in$ F18 by rules for constant functions, the identity function, sum, and composition with sine.

This proves that the induction hypothesis holds in the Base cases.

Constructor Cases: ($f^{(-1)}$). Assume $f, df/dx \in$ F18 to prove $d\,f^{(-1)}(x)/dx \in$ F18. Letting $y = f(x)$, so $x = f^{(-1)}(y)$, we know from Leibniz's rule in calculus that

$$df^{(-1)}(y)/dy = dx/dy = \frac{1}{dy/dx}. \tag{1}$$

For example,

$$d\sin^{(-1)}(y)/dy = 1/(d\sin(x)/dx) = 1/\cos(x) = 1/\cos(\sin^{(-1)}(y)).$$

Stated as in (1), this rule is easy to remember, but can easily be misleading because of the variable switching between x and y. It's more clearly stated using variable-free notation:

$$(f^{(-1)})' = (1/f') \circ f^{(-1)}. \tag{2}$$

Now, since $f' \in$ F18 (by assumption), so is $1/f'$ (by part (a)) and $f^{(-1)}$ (by constructor rule 2.), and therefore so is their composition (by rule 3). Hence the righthand side of equation (2) defines a function in F18.

Constructor Case: ($f \circ g$). Assume $f, g, df/dx, dg/dx \in$ F18 to prove $d(f \circ g)(x)/dx \in$ F18.

The Chain Rule states that

$$\frac{d(f(g(x)))}{dx} = \frac{df(g)}{dg} \cdot \frac{dg}{dx}.$$

Stated more clearly in variable-free notation, this is

$$(f \circ g)' = (f' \circ g) \cdot g'.$$

The righthand side of this equation defines a function in F18 by constructor rules 3. and 1.

The other Constructor cases are similar, so we conclude that the induction hypothesis holds in all Constructor cases.

This completes the proof by structural induction that the statement holds for all $f \in$ F18. ■

Problem 2.

Let p be the string [ ]. A string of brackets is said to be *erasable* iff it can be reduced to the empty string by repeatedly erasing occurrences of p. For example, here's how to erase the string [[[ ]][ ]][ ]:

$$[[[\,]][\,]][\,] \to [[\,]] \to [\,] \to \lambda.$$

On the other hand the string [ ]][[[[[ ]] is not erasable because when we try to erase, we get stuck:

$$[\,]][[[[[\,]] \to][[[[\,] \to][[[\not\to$$

Let $textErasable$ be the set of erasable strings of brackets. Let $textRecMatch$ be the recursive data type of strings of *matched* brackets given in Definition **??**.

(a) Use structural induction to prove that

$$textRecMatch \subseteq textErasable.$$

Solution. *Proof.* We prove by structural induction on the definition of $textRecMatch$ that the predicate

$$P(x) ::= x \in textErasable$$

is true for all $x \in textRecMatch$.

Base case: ($x = \lambda$) The empty string is erasable by definition of $textErasable$ – it can be reduced to itself by erasing the substring [0 times.

Constructor case: ($x =$ [s] t for $s, t \in textRecMatch$). By structural induction hypothesis, we may assume that $s, t \in textErasable$. So to erase x, erase s and then erase t to be left with the substring [ ], and one more erasure leads to the empty string.

This completes the proof by structural induction, so we conclude that

$$\forall x.\ x \in textRecMatch \quad \text{IMPLIES} \quad x \in textErasable$$

which by definition means that $textRecMatch \subseteq textErasable$.

■

(b) Supply the missing parts of the following proof that

$$textErasable \subseteq textRecMatch.$$

Proof. We prove by induction on the length, n, of strings, x, that if $x \in textErasable$, then $x \in textRecMatch$. The induction predicate is

$$P(n) ::= \forall x \in textErasable.\ (|x| \leq n \quad \text{IMPLIES} \quad x \in textRecMatch)$$

Base case:

What is the base case? Prove that P is true in this case.

Solution. The base case is ($n = 0$). Now $P(0)$ is true because the empty string is the only string of length 0, and it is in $textRecMatch$ by the base case of Definition **??** of $textRecMatch$. ■

Inductive step: To prove $P(n+1)$, suppose $|x| \leq n+1$ and $x \in textErasable$. We need only show that $x \in textRecMatch$. Now if $|x| < n+1$, then the induction hypothesis, $P(n)$, implies that $x \in textRecMatch$, so we only have to deal with x of length exactly $n+1$.

Let's say that a string y is an *erase* of a string z iff y is the result of erasing a single occurrence of p in z.

Since $x \in textErasable$ and has positive length, there must be an erase, $y \in textErasable$, of x. So $|y| = n-1$, and since $y \in textErasable$, we may assume by induction hypothesis that $y \in textRecMatch$.

Now we argue by cases:

Case (y is the empty string).

Prove that $x \in textRecMatch$ in this case.

Solution. In this case $x = p \in textRecMatch$. ■

Case ($y =$ [s] t for some strings $s, t \in textRecMatch$.) Now we argue by subcases.

- **Subcase** (x is of the form [s'] t where s is an erase of s').
  Since $s \in textRecMatch$, it is erasable by part (b), which implies that $s' \in textErasable$. But $|s'| < |x|$, so by induction hypothesis, we may assume that $s' \in textRecMatch$. This shows that x is the result of the constructor step of $textRecMatch$, and therefore $x \in textRecMatch$.
- **Subcase** (x is of the form [s] t' where t is an erase of t').
  Prove that $x \in textRecMatch$ **in this subcase.**

  Solution. The proof is essentially identical to the previous case, with t, t' in place of s, s':
  Now t is erasable by part (b), so $t' \in textErasable$. But $|t'| < |x|$, so by induction hypothesis, we may assume that $t' \in textRecMatch$. This proves that x is the result of the constructor step of $textRecMatch$ and therefore $x \in textRecMatch$.

  ■

- **Subcase**($x = p$[s] t).
  Prove that $x \in textRecMatch$ **in this subcase.**

  Solution. Let $t' ::=$ [s] t and s' be the empty string. Then $x =$ [s'] t'. But we know $s', t' \in textRecMatch$, which implies that $x \in textRecMatch$ because it is the result the $textRecMatch$ constructor step applied to s', t'. ■

The proofs of the remaining subcases are just like this last one. **List these remaining subcases.**

Solution.

- **case** ($x =$ [ps] t),
- **case** ($x =$ [sp] t),
- **case** ($x =$ [s] pt),
- **case** ($x =$ [s] tp).

■

This completes the proof by induction on n, so we conclude that $P(n)$ holds for all $n \in \mathbb{N}$. Therefore $x \in textRecMatch$ for every string $x \in textErasable$. That is,

$$textErasable \subseteq textRecMatch \text{ and hence } textErasable = textRecMatch.$$

■

Problem 3.
Here is a simple recursive definition of the set, E, of even integers:

Definition. Base case: $0 \in E$.

Constructor cases: If $n \in E$, then so are $n + 2$ and $-n$.

Provide similar simple recursive definitions of the following sets:

(a) The set $S ::= \{2^k 3^m 5^n \mid k, m, n \in \mathbb{N}\}$.

Solution. We can define the set S recursively as follows:

- $1 \in S$
- If $n \in S$, then $2n$, $3n$, and $5n$ are in S.

■

(b) The set $T ::= \{2^k 3^{2k+m} 5^{m+n} \mid k, m, n \in \mathbb{N}\}$.

Solution. We can define the set T recursively as follows:

- $1 \in T$
- If $n \in S$, then $18n$, $15n$, and $5n$ are in T.

■

(c) The set $L ::= \{(a, b) \in \mathbb{Z}^2 \mid 3 \mid (a - b)\}$.

Solution. We can define a set $L' = L$ recursively as follows:

- $(0, 0), (1, 1), (2, 2) \in L'$
- If $(a, b) \in L'$, then $(a + 3, b)$, $(a - 3, b)$, $(a, b + 3)$, and $(a, b - 3)$ are in L'.

Lots of other definitions are also possible. ■

Let L' be the set defined by the recursive definition you gave for L in the previous part. Now if you did it right, then $L' = L$, but maybe you made a mistake. So let's check that you got the definition right.

(d) Prove by structural induction on your definition of L' that

$$L' \subseteq L.$$

Solution. For the L' defined above, a straightforward structural induction shows that if $(c, d) \in L'$, then $(c, d) \in L$. Namely, each of the base cases in the definition of L' are in L since $3 \mid 0$. For the constructor cases, we may assume $(a, b) \in L$, that is $3 \mid (a - b)$, and must prove that $(a \pm 3, b) \in L$ and $(a, b \pm 3) \in L$. In the first the case, we must show that $3 \mid ((a \pm 3) - b)$. But this follows immediately because $((a \pm 3) - b) = (a - b) \pm 3$ and 3 divides both $(a - b)$ and 3. The other constructor case $(a, b \pm 3)$ follows in exactly the same way. So we conclude by structural induction on the definition of L' that $L' \subseteq L$. ■

(e) Confirm that you got the definition right by proving that

$$L \subseteq L'.$$

Solution. Conversely, we must show that $L \subseteq L'$. So suppose $(c, d) \in L$, that is, $3 \mid (c - d)$. This means that $c = r + 3k$ and $d = r + 3j$ for some $r \in \{0, 1, 2\}$ and $j, k \in \mathbb{Z}$. Then starting from base case $(r, r) \in L'$, we can apply the $(a \pm 3, b)$ constructor rule $|k|$ times to conclude that $(c, r) \in L'$, and then apply the $(a, b \pm 3)$ rule $|j|$ times to conclude that $(c, d) \in L'$. This implies that $L \subseteq L'$, which completes the proof that $L = L'$. ■

(f) See if you can give an *unambiguous* recursive definition of L.

Solution. This is tricky. Here is an attempt:

base cases: $(0,0), (1,1), (2,2), (-1,-1), (-2,-2), (-3,-3)(1,-2), (2,-1), (-1,2), (-2,1) \in L$

Now the idea is to constrain the constructors so the two coordinates have absolute values that increase differing by at most 1, then one coordinate only can continue to grow in absolute value. Let

$$\text{Sg}(x) ::= \begin{cases} 1 \text{ if } x \geq 0, \\ -1 \text{ if } x < 0. \end{cases}$$

constructors: if $(a, b) \in L'$, then

- if $||a| - |b|| \leq 1$, then $(a + 3\text{Sg}(a), b + 3\text{Sg}(b)), (a + 3\text{Sg}(a), b), (a, b + 3\text{Sg}(b)) \in L'$,
- if $|a| > |b| + 1$, then $(a + 3\text{Sg}(a), b) \in L'$,
- if $|b| > |a| + 1$, then $(a, b + 3\text{Sg}(b)) \in L'$.

■

6.042J / 18.062J Mathematics for Computer Science
Spring 2010

Solutions to In-Class Problems Week 7, Fri.

Problem 1.
Figures 1–4 show different pictures of planar graphs.

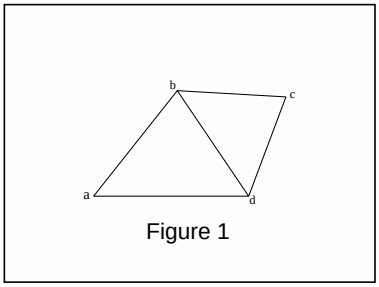


Figure 1

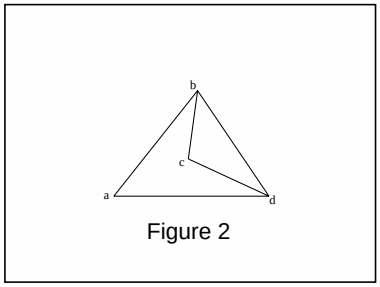


Figure 2

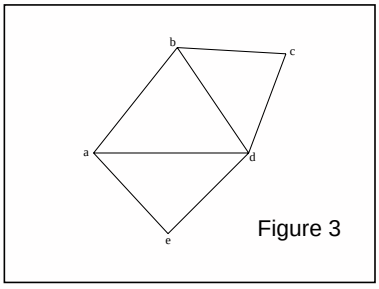


Figure 3

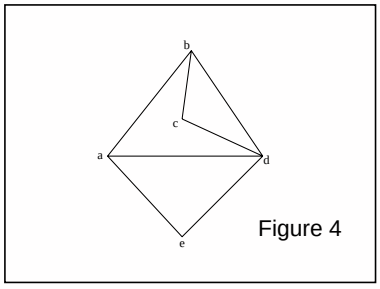


Figure 4

(a) For each picture, describe its discrete faces (simple cycles that define the region borders).

Solution. Figs 1 & 2: abda, bcdb, abcda. Fig 3: abcdea, adea,abda,bcdb. Fig 4: abcda, abdea, bdcb, adea. ■

(b) Which of the pictured graphs are isomorphic? Which pictures represent the same *planar embedding*? – that is, they have the same discrete faces.

Solution. Figs 1 & 2 have the same faces, so are different pictures of the *same* planar drawing. Figs 3 & 4 both have four faces, but they are different, for example, Fig 3 has a face with 5 edges, but the longest face in Fig 4 has 4 edges. ■

(c) Describe a way to construct the embedding in Figure 4 according to the recursive Definition 12.3.1 of planar embedding. For each application of a constructor rule, be sure to indicate the faces (cycles) to which the rule was applied and the cycles which result from the application.

Solution. Here's one way. (By Lemma 12.7.1, the constructor steps could be done in any order.)

recursive step		faces
vertex a	(base case)	a
vertex b	(base)	b
a—b	(bridge)	aba
vertex c	(base)	c
b—c	(bridge)	$abcba$
vertex d	(base)	d
c—d	(bridge)	$abcdcba$
a—d	(split)	$dabcd$, $dabcd$
b—d	(split)	$dabd$, $dbcd$, $abcda$
vertex e	(base)	e
d—e	(bridge)	$dedabd$, $dbcd$, $abcda$
a—e	(split)	$abdea$, $adea$, $dbcd$, $abcda$

■

Problem 2.
Prove the following assertions by structural induction on the definition of planar embedding.

(a) In a planar embedding of a graph, each edge is traversed a total of two times by the faces of the embedding.

Solution. *Proof.* The induction hypothesis is that if $\mathcal{E}$ is a planar embedding of a graph, then each edge is traversed exactly twice by the faces of $\mathcal{E}$.

Base case: There is one vertex and no edges, so this case holds vacuously.

Constructor case: (face-splitting) The only change is that one face of $\mathcal{E}$ splits into two new faces, each traversing the new edge once.

Constructor case: (bridge between two connected graphs) The only change is that two faces merge into one face that makes two traversals of the new bridging edge. So the traversals of other edges are unchanged, and the new edge is traversed twice by the new face.

So in any case, all edges of $\mathcal{E}$ are traversed exactly twice. This completes the proof of the Constructor case. We conclude by structural induction that for all planar embeddings, $\mathcal{E}$, then each edge is traversed exactly twice by the faces of $\mathcal{E}$.

■

(b) In a planar embedding of a connected graph with at least three vertices, each face is of length at least three.

Solution. *Proof.* The induction hypothesis is that if $\mathcal{E}$ is a planar embedding of a graph with at least three vertices, then all faces in $\mathcal{E}$ are of length at least three.

Base case: There is one vertex, so this case holds vacuously.

Constructor case: (face-splitting) An edge a—b is added between nonadjacent vertices a, b on the same face. This face is replaced by two new faces of the form $abc \ldots a$ and $abd \ldots a$ where $c \neq d$ are vertices different from a and b. So both new faces are of length at least 3; no other faces change.

Constructor case: (bridge between two connected graphs)

case 1: (both graphs have one vertex). Connecting these graphs with a bridge gives a graph with fewer than three vertices, so this case holds vacuously.

case 2: (one graph has exactly two vertices and the other has at most two vertices). Connecting these graphs with a bridge yields a line graph of length two or three whose unique embedding is a cycle of length four or six going from one end of the graph to the other and back. In any case, the one face has length more than three.

case 3: (one graph has at most two vertices and the other has at least three vertices). Connecting replaces the face of the vertex graph with at most two vertices and a face of the other graph with a face of length at least $2 + 3 = 5$, and leaves all other faces unchanged. So all faces are indeed of length at least three.

case 4: (both graphs have at least three vertices). Connecting replaces two faces of length at least three by a single face of length at least $2 + 3 + 3 = 7$, and leaves all other faces unchanged. So all faces are indeed of length at least three.

So in any case, all faces of connected planar embedding of graphs with at least three vertices are indeed of length at least three. This completes the proof of the Constructor case and the structural induction.

■

Problem 3. (a) Show that if a connected planar graph with more than two vertices is bipartite, then

$$e \leq 2v - 4. \tag{1}$$

Hint: Similar to the proof of Corollary 12.6.3 that for planar graphs $e \leq 3v - 6$.

Solution. By Problem 2.b, every face is of length at least 3. But in a bipartite graph there are no cycles of odd length, so all must be of length at least 4.

Each edge is traversed by exactly two faces, so

$$2e = \sum_{f \in \text{ faces}} \text{length}(f) \geq \sum_{f \in \text{ faces}} 4 = 4f. \tag{2}$$

By Euler's formula, $f = e - v + 2$, so substituting for f in (2), yields

$$2e \geq 4(e - v + 2),$$

which simplifies to (1).

■

(b) Conclude that that $K_{3,3}$ is not planar. ($K_{3,3}$ is the graph with six vertices and an edge from each of the first three vertices to each of the last three.)

Solution. $K_{3,3}$ is bipartite and connected. Also, it has 9 edges and 6 vertices, and since $9 > 8 = 2 \cdot 6 - 4$, it does not satisfy (1), and so cannot be planar. ■

Appendix

Definition 3.1. A *planar embedding* of a *connected* graph consists of a nonempty set of cycles of the graph called the *discrete faces* of the embedding. Planar embeddings are defined recursively as follows:

- **Base case:** If G is a graph consisting of a single vertex, v, then a planar embedding of G has one discrete face, namely the length zero cycle, v.
- **Constructor Case:** (split a face) Suppose G is a connected graph with a planar embedding, and suppose a and b are distinct, nonadjacent vertices of G that appear on some discrete face, γ, of the planar embedding. That is, γ is a cycle of the form

  $$a \ldots b \cdots a.$$

  Then the graph obtained by adding the edge a—b to the edges of G has a planar embedding with the same discrete faces as G, except that face γ is replaced by the two discrete faces[1]

  $$a \ldots ba \quad \text{and } ab \cdots a,$$

  as illustrated in Figure 1.

[1] There is one exception to this rule. If G is a line graph beginning with a and ending with b, then the cycles into which γ splits are actually the same. That's because adding edge a—b creates a simple cycle graph, C_n, that divides the plane into an "inner" and an "outer" region with the same border. In order to maintain the correspondence between continuous faces and discrete faces, we have to allow two "copies" of this same cycle to count as discrete faces. But since this is the only situation in which two faces are actually the same cycle, this exception is better explained in a footnote than mentioned explicitly in the definition.

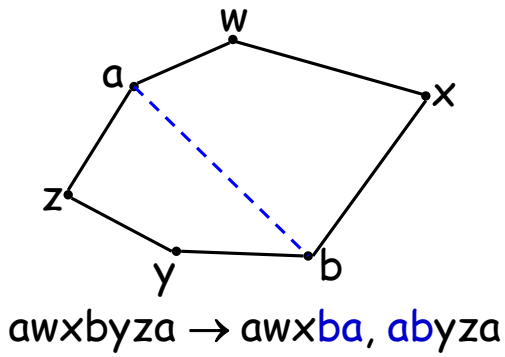


Figure 1: The Split a Face Case.

- **Constructor Case:** (add a bridge) Suppose G and H are connected graphs with planar embeddings and disjoint sets of vertices. Let a be a vertex on a discrete face, γ, in the embedding of G. That is, γ is of the form

  $$a \ldots a.$$

  Similarly, let b be a vertex on a discrete face, δ, in the embedding of H, so δ is of the form

  $$b \cdots b.$$

  Then the graph obtained by connecting G and H with a new edge, a—b, has a planar embedding whose discrete faces are the union of the discrete faces of G and H, except that faces γ and δ are replaced by one new face

  $$a \ldots ab \cdots ba,$$

  as illustrated in Figure 2.

An arbitrary graph is *planar* iff each of its connected components has a planar embedding.

Theorem 3.2 (Euler's Formula)**.** *If a connected graph has a planar embedding, then*

$$v - e + f = 2$$

where v is the number of vertices, e is the number of edges, and f is the number of faces.

Corollary 3.3. *Suppose a connected planar graph has $v \geq 3$ vertices and e edges. Then*

$$e \leq 3v - 6.$$

Proof. By definition, a connected graph is planar iff it has a planar embedding. So suppose a connected graph with v vertices and e edges has a planar embedding with f faces. By Problem 2.a, every edge is traversed exactly twice by the face boundaries. So the sum of the lengths of the face

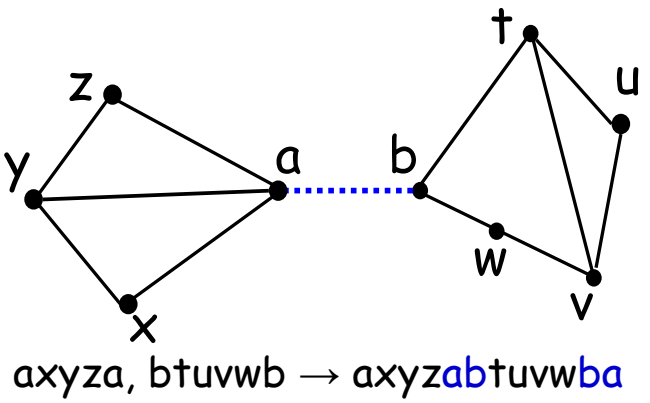


Figure 2: The Add Bridge Case.

boundaries is exactly $2e$. Also by Problem 2.b, when $v \geq 3$, each face boundary is of length at least three, so this sum is at least $3f$. This implies that

$$3f \leq 2e. \tag{3}$$

But $f = e - v + 2$ by Euler's formula, and substituting into (3) gives

$$\begin{aligned} 3(e - v + 2) &\leq 2e \\ e - 3v + 6 &\leq 0 \\ e &\leq 3v - 6 \end{aligned}$$

■

Corollary 3.4. *K_5 is not planar.*

Proof.

$$e = 10 > 9 = 3v - 6.$$

■

6.042J / 18.062J Mathematics for Computer Science
Spring 2010

Solutions to In-Class Problems Week 8, Mon.

Problem 1.
A number is *perfect* if it is equal to the sum of its positive divisors, other than itself. For example, 6 is perfect, because $6 = 1 + 2 + 3$. Similarly, 28 is perfect, because $28 = 1 + 2 + 4 + 7 + 14$. Explain why $2^{k-1}(2^k - 1)$ is perfect when $2^k - 1$ is prime.[1]

Solution. If $2^k - 1$ is prime, then the only divisors of $2^{k-1}(2^k - 1)$ are:

$$1, \quad 2, \quad 4, \quad \ldots, \quad 2^{k-1}, \tag{1}$$

and

$$1 \cdot (2^k - 1), \quad 2 \cdot (2^k - 1), \quad 4 \cdot (2^k - 1), \quad \ldots, \quad 2^{k-2} \cdot (2^k - 1). \tag{2}$$

The sequence (1) sums to $2^k - 1$ (using the formula for a geometric series,[2] and likewise the sequence (2) sums to $(2^{k-1} - 1) \cdot (2^k - 1)$. Adding these two sums gives $2^{k-1}(2^k - 1)$, so the number is perfect. ■

Problem 2. (a) Use the Pulverizer to find integers x, y such that

$$x \cdot 50 + y \cdot 21 = \gcd(50, 21).$$

[1] Euclid proved this 2300 years ago. About 250 years ago, Euler proved the converse: *every* even perfect number is of this form (for a simple proof see http://primes.utm.edu/notes/proofs/EvenPerfect.html). As is typical in number theory, apparently simple results lie at the brink of the unknown. For example, it is not known if there are an infinite number of even perfect numbers or any odd perfect numbers at all.

[2] It's fun to notice the "Computer Science" proof that (1) sums to $2^k - 1$. The binary binary representation of 2^j is a 10^j, so the sum is represented by 1^k. This what you get by subtracting 1 from by 10^k which is the binary representation of 2^k.

Solution. Here is the table produced by the Pulverizer:

x	y	$\text{rem}(x,y)$	$=$	$x - q \cdot y$
50	21	8	$=$	$50 - 2 \cdot 21$
21	8	5	$=$	$21 - 2 \cdot 8$
			$=$	$21 - 2 \cdot (50 - 2 \cdot 21)$
			$=$	$-2 \cdot 50 + 5 \cdot 21$
8	5	3	$=$	$8 - 1 \cdot 5$
			$=$	$(50 - 2 \cdot 21) - 1 \cdot (-2 \cdot 50 + 5 \cdot 21)$
			$=$	$3 \cdot 50 - 7 \cdot 21$
5	3	2	$=$	$5 - 1 \cdot 3$
			$=$	$(-2 \cdot 50 + 5 \cdot 21) - 1 \cdot (3 \cdot 50 - 7 \cdot 21)$
			$=$	$-5 \cdot 50 + 12 \cdot 21$
3	2	1	$=$	$3 - 1 \cdot 2$
			$=$	$(3 \cdot 50 - 7 \cdot 21) - 1 \cdot (-5 \cdot 50 + 12 \cdot 21)$
			$=$	$\boxed{8 \cdot 50 - 19 \cdot 21}$
2	1	0		

■

(b) Now find integers x', y' with $y' > 0$ such that

$$x' \cdot 50 + y' \cdot 21 = \gcd(50, 21)$$

Solution. since $(x, y) = (8, -19)$ works, so does $(8 - 21n, -19 + 50n)$ for any $n \in \mathbb{Z}$, so letting $n = 1$, we have

$$-13 \cdot 50 + 31 \cdot 21 = 1$$

■

Problem 3.
For nonzero integers, a, b, prove the following properties of divisibility and GCD'S. (You may use the fact that $\gcd(a, b)$ is an integer linear combination of a and b. You may not appeal to uniqueness of prime factorization because the properties below are needed to *prove* unique factorization.)

(a) Every common divisor of a and b divides $\gcd(a, b)$.

Solution. For some s and t, $\gcd(a, b) = sa + tb$. Let c be a common divisor of a and b. Since $c \mid a$ and $c \mid b$, we have $a = kc, b = k'c$ so

$$sa + tb = skc + tk'c = c(sk + tk')$$

so $c \mid sa + tb$. ■

(b) If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.

Solution. Since $\gcd(a, b) = 1$, we have $sa + tb = 1$ for some s, t. Multiplying by c, we have

$$sac + tbc = c$$

but a divides the second term of the sum since $a \mid bc$, and it obviously divides the first term, and therefore it divides the sum, which equals c.

■

(c) If $p \mid ab$ for some prime, p, then $p \mid a$ or $p \mid b$.

Solution. If p does not divide a, then since p is prime, $\gcd(p, a) = 1$. By part (b), we conclude that $p \mid b$. ■

(d) Let m be the smallest integer linear combination of a and b that is positive. Show that $m = \gcd(a, b)$.

Solution. Since $\gcd(a, b)$ is positive and an integer linear common of a and b, we have

$$m \leq \gcd(a, b).$$

On the other hand, since m is a linear combination of a and b, every common factor of a and b divides m. So in particular, $\gcd(a, b) \mid m$, which implies

$$\gcd(a, b) \leq m.$$

■

Appendix: The Pulverizer

Euclid's algorithm for finding the GCD of two numbers relies on repeated application of the equation:

$$\gcd(a, b) = \gcd(b, \text{rem}(a, b))$$

For example, we can compute the GCD of 259 and 70 as follows:

$$\begin{aligned}
\gcd(259, 70) &= \gcd(70, 49) && \text{since } \text{rem}(259, 70) = 49 \\
&= \gcd(49, 21) && \text{since } \text{rem}(70, 49) = 21 \\
&= \gcd(21, 7) && \text{since } \text{rem}(49, 21) = 7 \\
&= \gcd(7, 0) && \text{since } \text{rem}(21, 7) = 0 \\
&= 7.
\end{aligned}$$

The Pulverizer goes through the same steps, but requires some extra bookkeeping along the way: as we compute $\gcd(a, b)$, we keep track of how to write each of the remainders (49, 21, and 7, in the example) as a linear combination of a and b (this is worthwhile, because our objective is to write

the last nonzero remainder, which is the GCD, as such a linear combination). For our example, here is this extra bookkeeping:

x	y	$\text{rem}(x, y)$	$=$	$x - q \cdot y$
259	70	49	$=$	$259 - 3 \cdot 70$
70	49	21	$=$	$70 - 1 \cdot 49$
			$=$	$70 - 1 \cdot (259 - 3 \cdot 70)$
			$=$	$-1 \cdot 259 + 4 \cdot 70$
49	21	7	$=$	$49 - 2 \cdot 21$
			$=$	$(259 - 3 \cdot 70) - 2 \cdot (-1 \cdot 259 + 4 \cdot 70)$
			$=$	$\boxed{3 \cdot 259 - 11 \cdot 70}$
21	7	0		

We began by initializing two variables, $x = a$ and $y = b$. In the first two columns above, we carried out Euclid's algorithm. At each step, we computed $\text{rem}(x, y)$, which can be written in the form $x - q \cdot y$. (Remember that the Division Algorithm says $x = q \cdot y + r$, where r is the remainder. We get $r = x - q \cdot y$ by rearranging terms.) Then we replaced x and y in this equation with equivalent linear combinations of a and b, which we already had computed. After simplifying, we were left with a linear combination of a and b that was equal to the remainder as desired. The final solution is boxed.

6.042J / 18.062J Mathematics for Computer Science
Spring 2010

Solutions to In-Class Problems Week 8, Wed.

Problem 1. (a) Use the Pulverizer to find the inverse of 13 modulo 23 in the range $\{1, \ldots, 22\}$.

Solution. We first use the Pulverizer to find s, t such that $\gcd(23, 13) = s \cdot 23 + t \cdot 13$, namely,

$$1 = 4 \cdot 23 - 7 \cdot 13.$$

This implies that -7 is an inverse of 13 modulo 23.

Here is the Pulverizer calculation:

x	y	$\text{rem}(x, y)$	$=$	$x - q \cdot y$
23	13	10	$=$	$23 - 13$
13	10	3	$=$	$13 - 10$
			$=$	$13 - (23 - 13)$
			$=$	$(-1) \cdot 23 + 2 \cdot 13$
10	3	1	$=$	$10 - 3 \cdot 3$
			$=$	$(23 - 13) - 3 \cdot ((-1) \cdot 23 + 2 \cdot 13))$
			$=$	$\boxed{4 \cdot 23 - 7 \cdot 13}$
3	1	0	$=$	

To get an inverse in the specified range, simply find $\text{rem}(-7, 23)$, namely **16**.

■

(b) Use Fermat's theorem to find the inverse of 13 modulo 23 in the range $\{1, \ldots, 22\}$.

Solution. Since 23 is prime, Fermat's theorem implies $13^{23-2} \cdot 13 \equiv 1 \pmod{23}$ and so $\text{rem}(13^{23-2}, 23)$ is the inverse of 13 in the range $\{1, \ldots, 22\}$. Now using the method of repeated squaring, we have

the following congruences modulo 23:

$$\begin{aligned}
13^2 &= 169 \\
&\equiv \text{rem}(169, 23) = 8 \\
\\
13^4 &\equiv 8^2 \\
&= 64 \\
&\equiv \text{rem}(64, 23) = 18 \\
\\
13^8 &\equiv 18^2 \\
&= 324 \\
&\equiv \text{rem}(324, 23) = 2 \\
\\
13^{16} &\equiv 2^2 \\
&= 4 \\
\\
13^{21} &= 13^{16} \cdot 13^4 \cdot 13 \\
&\equiv 4 \cdot 18 \cdot 13 \\
&= (4 \cdot 6) \cdot (3 \cdot 13) \\
&= 24 \cdot 39 \\
&\equiv 1 \cdot 39 \\
&\equiv \text{rem}(39, 23) = \boxed{16}.
\end{aligned}$$

■

Problem 2. (a) Why is a number written in decimal evenly divisible by 9 if and only if the sum of its digits is a multiple of 9? *Hint:* $10 \equiv 1 \pmod 9$.

Solution. Since $10 \equiv 1 \pmod 9$, so is

$$10^k \equiv 1^k \equiv 1 \pmod 9. \tag{1}$$

Now a number in decimal has the form:

$$d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \ldots + d_1 \cdot 10 + d_0.$$

From (1), we have

$$d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \ldots + d_1 \cdot 10 + d_0 \equiv d_k + d_{k-1} + \ldots + d_1 + d_0 \pmod 9$$

This shows something stronger than what we were asked to show, namely, it shows that the remainder when the original number is divided by 9 is equal to the remainder when the sum of the digits is divided by 9. In particular, if one is zero, then so is the other. ■

(b) Take a big number, such as 37273761261. Sum the digits, where every other one is negated:

$$3 + (-7) + 2 + (-7) + 3 + (-7) + 6 + (-1) + 2 + (-6) + 1 = -11$$

Explain why the original number is a multiple of 11 if and only if this sum is a multiple of 11.

Solution. A number in decimal has the form:

$$d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \ldots + d_1 \cdot 10 + d_0$$

Observing that $10 \equiv -1 \pmod{11}$, we know:

$$\begin{aligned} & d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \cdots + d_1 \cdot 10 + d_0 \\ & \equiv d_k \cdot (-1)^k + d_{k-1} \cdot (-1)^{k-1} + \cdots + d_1 \cdot (-1)^1 + d_0 \cdot (-1)^0 \pmod{11} \\ & \equiv d_k - d_{k-1} + \cdots - d_1 + d_0 \pmod{11} \end{aligned}$$

assuming k is even. The case where k is odd is the same with signs reversed.

The procedure given in the problem computes $\pm$ this alternating sum of digits, and hence yields a number divisible by 11 ($\equiv 0 \pmod{11}$) iff the original number was divisible by 11. ■

Problem 3.
The following properties of equivalence mod n follow directly from its definition and simple properties of divisibility. See if you can prove them without looking up the proofs in the text.

(a) If $a \equiv b \pmod{n}$, then $ac \equiv bc \pmod{n}$.

Solution. The condition $a \equiv b \pmod{n}$ is equivalent to the assertion $n \mid (a - b)$. This implies that $n \mid (a - b)c$, and so $n \mid (ac - bc)$. This is equivalent to $ac \equiv bc \pmod{n}$. ■

(b) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

Solution. Assume $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, that is, $n \mid (a - b)$ and $n \mid (b - c)$. Then $n \mid (a - b) + (b - c) = (a - c)$, so $a \equiv c \pmod{n}$. ■

(c) If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $ac \equiv bd \pmod{n}$.

Solution. $a \equiv b \pmod{n}$ implies $ac \equiv bc \pmod{n}$ by part (a); likewise, $c \equiv d \pmod{n}$ implies $bc \equiv bd \pmod{n}$. So $ac \equiv bd \pmod{n}$ by part (b). ■

(d) $\text{rem}(a, n) \equiv a \pmod{n}$.

Solution. The remainder $\text{rem}(a, n)$ is equal to $a - qn$ for some integer q. However, for every integer q:

$$\begin{aligned} n \mid qn \quad & \text{IFF} \quad n \mid ((a - qn) - a) \\ & \text{IMPLIES} \quad n \mid (\text{rem}(a, n) - a) \\ & \text{IFF} \quad \text{rem}(a, n) \equiv a \pmod{n}. \end{aligned}$$

■

6.042J / 18.062J Mathematics for Computer Science
Spring 2010

Solutions to In-Class Problems Week 8, Fri.

Problem 1.
Let's try out RSA! There is a complete description of the algorithm at the bottom of the page. You'll probably need extra paper. **Check your work carefully!**

(a) As a team, go through the **beforehand** steps.

- Choose primes p and q to be relatively small, say in the range 10-40. In practice, p and q might contain several hundred digits, but small numbers are easier to handle with pencil and paper.
- Try $e = 3, 5, 7, \ldots$ until you find something that works. Use Euclid's algorithm to compute the gcd.
- Find d (using the Pulverizer —see appendix for a reminder on how the Pulverizer works —or Euler's Theorem).

When you're done, put your public key on the board. This lets another team send you a message.

(b) Now send an encrypted message to another team using their public key. Select your message m from the codebook below:

- 2 = Greetings and salutations!
- 3 = Yo, wassup?
- 4 = You guys are slow!
- 5 = All your base are belong to us.
- 6 = Someone on *our* team thinks someone on *your* team is kinda cute.
- 7 = You *are* the weakest link. Goodbye.

(c) Decrypt the message sent to you and verify that you received what the other team sent!

RSA Public Key Encryption

Beforehand The receiver creates a public key and a secret key as follows.

1. Generate two distinct primes, p and q.
2. Let $n = pq$.
3. Select an integer e such that $\gcd(e, (p-1)(q-1)) = 1$.
   The *public key* is the pair (e, n). This should be distributed widely.
4. Compute d such that $de \equiv 1 \pmod{(p-1)(q-1)}$.
   The *secret key* is the pair (d, n). This should be kept hidden!

Encoding The sender encrypts message m, where $0 \leq m < n$, to produce m' using the public key:

$$m' = \text{rem}(m^e, n).$$

Decoding The receiver decrypts message m' back to message m using the secret key:

$$m = \text{rem}((m')^d, n).$$

Problem 2.
A critical fact about RSA is, of course, that decrypting an encrypted message always gives back the original message! That is, that $\text{rem}((m^d)^e, pq) = m$. This will follow from something slightly more general:

Lemma 2.1. *Let n be a product of distinct primes and $a \equiv 1 \pmod{\phi(n)}$ for some nonnegative integer, a. Then*

$$m^a \equiv m \pmod{n}. \tag{1}$$

(a) Explain why Lemma 2.1 implies that k and k^5 have the same last digit. For example:

$$\underline{2}^5 = 3\underline{2} \qquad\qquad 7\underline{9}^5 = 3077056399$$

Hint: What is $\phi(10)$?

Solution. Two nonnegative integers have the same last digit iff they are $\equiv \pmod{10}$. Now $\phi(10) = \phi(2)\phi(5) = 4$ and $5 \equiv 1 \pmod{4}$, so by Lemma 2.1,

$$k^5 \equiv k \pmod{10}.$$

■

(b) Explain why Lemma 2.1 implies that the original message, m, equals $\text{rem}((m^e)^d, pq)$.

Solution. To apply Lemma 2.1 to RSA, note that the first condition of the Lemma is that n be a product of primes. In RSA, $n = pq$ so this condition holds.

For $n = pq$, the Euler function equations (see the Appendix) imply that $\phi(n) = (p-1)(q-1)$. So when d and e are chosen according to RSA, $de \equiv 1 \pmod{\phi(n)}$. So $a ::= de$ satisfies the second condition of the Lemma.

Now, from equation (1) with $n = pq$ and $a = de$, we have

$$(m^e)^d = m^{de} \equiv m \pmod{pq}.$$

Hence,

$$\text{rem}((m^e)^d, pq) = \text{rem}(m, pq),$$

but $\text{rem}(m, pq) = m$, since $0 \leq m < pq$. ■

(c) Prove that if p is prime, then

$$m^a \equiv m \pmod{p} \tag{2}$$

for all nonnegative integers $a \equiv 1 \pmod{p-1}$.

Solution. If $p \mid m$, then equation (2) holds since both sides of the congruence are $\equiv 0 \pmod{p}$.

So assume p does not divide m. Now if $a \equiv 1 \pmod{p-1}$, then $a = 1 + (p-1)k$ for some k, so

$$\begin{aligned} m^a &= m^{1+(p-1)k} \\ &= m \cdot \left(m^{p-1}\right)^k \\ &\equiv m \cdot (1)^k \pmod{p} && \text{(by Fermat's Little Thm.)} \\ &\equiv m \pmod{p}. \end{aligned}$$

■

(d) Prove that if n is a product of distinct primes, and $a \equiv b \pmod{p}$ for all prime factors, p, of n, then $a \equiv b \pmod{n}$.

Solution. By definition of congruence, $a \equiv b \pmod{k}$ iff $k \mid (a-b)$. So if $a \equiv b \pmod{p}$ for each prime factor, p, of n, then $p \mid (a-b)$ for each prime factor, p, and hence, so does their product (by the Unique Factorization Theorem). That is, $n \mid (a-b)$, which means $a \equiv b \pmod{n}$. ■

(e) Combine the previous parts to complete the proof of Lemma 2.1.

Solution. Suppose n is a product of distinct primes, $p_1 p_2 \cdots p_k$. Then from the formulas for the Euler function, ϕ, we have

$$\phi(n) = (p_1 - 1)(p_2 - 1) \cdots (p_k - 1).$$

Now suppose $a \equiv 1 \pmod{\phi(n)}$, that is, a is 1 plus a multiple of $\phi(n)$, so it is also 1 plus a multiple of $p_i - 1$. That is,

$$a \equiv 1 \pmod{p_i - 1}.$$

Hence, by part (c),

$$m^a \equiv m \pmod{p_i}$$

for all m. Since this holds for all factors, p_i, of n, we conclude from part (d) that

$$m^a \equiv m \pmod{n},$$

which proves Lemma 2.1. ■

Appendix

Inverses, Fermat, Euler

Lemma (Inverses mod n)**.** *If k and n are relatively prime, then there is integer k' called the* modulo n inverse *of k, such that*

$$k \cdot k' \equiv 1 \pmod{n}.$$

Remark: If $\gcd(k, n) = 1$, then $sk + tn = 1$ for some s, t, so we can choose $k' ::= s$ in the previous Lemma. So given k and n, an inverse k' can be found efficiently using the Pulverizer.

Theorem (Fermat's (Little) Theorem)**.** *If p is prime and k is not a multiple of p, then*

$$k^{p-1} \equiv 1 \pmod{p}$$

Definition. The value of *Euler's totient function*, $\phi(n)$, is defined to be the number of positive integers less than n that are relatively prime to n.

Lemma (Euler Totient Function Equations)**.**

$$\begin{aligned} \phi(p^k) &= p^k - p^{k-1} && \text{for prime, } p, \text{ and } k > 0, \\ \phi(mn) &= \phi(m) \cdot \phi(n) && \text{when } \gcd(m, n) = 1. \end{aligned}$$

Theorem (Euler's Theorem)**.** *If k and n are relatively prime, then*

$$k^{\phi(n)} \equiv 1 \pmod{n}$$

Corollary. *If k and n are relatively prime, then $k^{\phi(n)-1}$ is an inverse modulo n of k.*

Remark: Using fast exponentiation to compute $k^{\phi(n)-1}$ is another efficient way to compute an inverse modulo n of k.

The Pulverizer

Euclid's algorithm for finding the GCD of two numbers relies on repeated application of the equation:

$$\gcd(a, b) = \gcd(b, \text{rem}(a, b))$$

For example, we can compute the GCD of 259 and 70 as follows:

$$\begin{aligned} \gcd(259, 70) &= \gcd(70, 49) && \text{since } \text{rem}(259, 70) = 49 \\ &= \gcd(49, 21) && \text{since } \text{rem}(70, 49) = 21 \\ &= \gcd(21, 7) && \text{since } \text{rem}(49, 21) = 7 \\ &= \gcd(7, 0) && \text{since } \text{rem}(21, 7) = 0 \\ &= 7. \end{aligned}$$

The Pulverizer goes through the same steps, but requires some extra bookkeeping along the way: as we compute $\gcd(a, b)$, we keep track of how to write each of the remainders (49, 21, and 7, in the example) as a linear combination of a and b (this is worthwhile, because our objective is to write

the last nonzero remainder, which is the GCD, as such a linear combination). For our example, here is this extra bookkeeping:

x	y	$\text{rem}(x, y)$	$=$	$x - q \cdot y$
259	70	49	$=$	$259 - 3 \cdot 70$
70	49	21	$=$	$70 - 1 \cdot 49$
			$=$	$70 - 1 \cdot (259 - 3 \cdot 70)$
			$=$	$-1 \cdot 259 + 4 \cdot 70$
49	21	7	$=$	$49 - 2 \cdot 21$
			$=$	$(259 - 3 \cdot 70) - 2 \cdot (-1 \cdot 259 + 4 \cdot 70)$
			$=$	$\boxed{3 \cdot 259 - 11 \cdot 70}$
21	7	0		

We began by initializing two variables, $x = a$ and $y = b$. In the first two columns above, we carried out Euclid's algorithm. At each step, we computed $\text{rem}(x, y)$, which can be written in the form $x - q \cdot y$. (Remember that the Division Algorithm says $x = q \cdot y + r$, where r is the remainder. We get $r = x - q \cdot y$ by rearranging terms.) Then we replaced x and y in this equation with equivalent linear combinations of a and b, which we already had computed. After simplifying, we were left with a linear combination of a and b that was equal to the remainder as desired. The final solution is boxed.

6.042J / 18.062J Mathematics for Computer Science
Spring 2010

Solutions to In-Class Problems Week 9, Mon.

Problem 1.
An explorer is trying to reach the Holy Grail, which she believes is located in a desert shrine d days walk from the nearest oasis. In the desert heat, the explorer must drink continuously. She can carry at most 1 gallon of water, which is enough for 1 day. However, she is free to create water caches out in the desert.

For example, if the shrine were $2/3$ of a day's walk into the desert, then she could recover the Holy Grail with the following strategy. She leaves the oasis with 1 gallon of water, travels $1/3$ day into the desert, caches $1/3$ gallon, and then walks back to the oasis— arriving just as her water supply runs out. Then she picks up another gallon of water at the oasis, walks $1/3$ day into the desert, tops off her water supply by taking the $1/3$ gallon in her cache, walks the remaining $1/3$ day to the shine, grabs the Holy Grail, and then walks for $2/3$ of a day back to the oasis— again arriving with no water to spare.

But what if the shrine were located farther away?

(a) What is the most distant point that the explorer can reach and then return to the oasis if she takes only 1 gallon from the oasis?

Solution. At best she can walk $1/2$ day into the desert and then walk back. ■

(b) What is the most distant point the explorer can reach and still return to the oasis if she takes only 2 gallons from the oasis? No proof is required; just do the best you can.

Solution. The explorer walks $1/4$ day into the desert, drops $1/2$ gallon, then walks home. Next, she walks $1/4$ day into the desert, picks up $1/4$ gallon from her cache, walks an additional $1/2$ day out and back, then picks up another $1/4$ gallon from her cache and walks home. Thus, her maximum distance from the oasis is $3/4$ of a day's walk. ■

(c) The explorer will travel using a recursive strategy to go far into the desert and back drawing a total of n gallons of water from the oasis. Her strategy is to build up a cache of $n-1$ gallons, plus enough to get home, a certain fraction of a day's distance into the desert. On the last delivery to the cache, instead of returning home, she proceeds recursively with her $n-1$ gallon strategy to go farther into the desert and return to the cache. At this point, the cache has just enough water left to get her home.

Prove that with n gallons of water, this strategy will get her $H_n/2$ days into the desert and back, where H_n is the nth Harmonic number:

$$H_n ::= \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}.$$

Conclude that she can reach the shrine, however far it is from the oasis.

Solution. To build up the first cache of $n-1$ gallons, she should make n trips $1/(2n)$ days into the desert, dropping off $(n-1)/n$ gallons each time. Before she leaves the cache for the last time, she has $n-1$ gallons plus enough for the walk home. Then she applies her $(n-1)$-day strategy. So letting D_n be her maximum distance into the desert and back, we have

$$D_n = \frac{1}{2n} + D_{n-1}.$$

So

$$\begin{aligned} D_n &= \frac{1}{2n} + \frac{1}{2(n-1)} + \frac{1}{2(n-2)} + \cdots + \frac{1}{2\cdot 2} + \frac{1}{2\cdot 1} \\ &= \frac{1}{2}\left(\frac{1}{n} + \frac{1}{(n-1)} + \frac{1}{(n-2)} + \cdots + \frac{1}{\cdot 2} + \frac{1}{\cdot 1}\right) \\ &= \frac{H_n}{2}. \end{aligned}$$

■

(d) Suppose that the shrine is $d = 10$ days walk into the desert. Use the asymptotic approximation $H_n \sim \ln n$ to show that it will take more than a million years for the explorer to recover the Holy Grail.

Solution. She obtains the Grail when:

$$\frac{H_n}{2} \approx \frac{\ln n}{2} \geq 10.$$

This requires $n \geq e^{20} = 4.8 \cdot 10^8$ days $> 1.329M$ years.

■

Problem 2.
There is a number a such that $\sum_{i=1}^{\infty} i^p$ converges iff $p < a$. What is the value of a? Prove it.

Solution. $a = -1$.

For $p = -1$, the sum is the harmonic series which we know does not converge. Since the term i^p is increasing in p for $i > 1$, the sum will be larger, and hence also diverge for $p > -1$.

For $p < -1$ there exists an $\epsilon > 0$ such that $p = -(1+\epsilon)$. By the integral method,

$$\begin{aligned} \sum_{i=1}^{\infty} i^{-(1+\epsilon)} &\leq 1 + \int_1^{\infty} x^{-(1+\epsilon)}\, dx \\ &= 1 + \epsilon^{-1} - \epsilon^{-1} \lim_{\alpha\to\infty} \alpha^{-\epsilon} \\ &= 1 + \epsilon^{-1} \\ &< \infty \end{aligned}$$

Hence the sum is bounded above, and since it is increasing, it has a finite limit, that is, it converges.

■

Problem 3.
Suppose $f, g : \mathbb{R} \to \mathbb{R}$ and $f \sim g$.

(a) Prove that $2f \sim 2g$.

$$\frac{2f}{2g} = \frac{f}{g},$$

so they have the same limit as $n \to \infty$.

(b) Prove that $f^2 \sim g^2$.

Solution.

$$\lim_{n\to\infty} \frac{f^2}{g^2} = \lim_{n\to\infty} \frac{f}{g} \cdot \frac{f}{g} = \lim_{n\to\infty} \frac{f}{g} \cdot \lim_{n\to\infty} \frac{f}{g} = 1 \cdot 1 = 1.$$

■

(c) Give examples of f and g such that $2^f \not\sim 2^g$.

Solution. Let $f(n) ::= n,\ g(n) ::= n + \log n$. Then

$$\frac{2^{f(n)}}{2^{g(n)}} = \frac{2^n}{2^{n+\log n}} = \frac{2^n}{2^n 2^{\log n}} = \frac{1}{n},$$

so

$$\lim_{n\to\infty} \frac{2^{f(n)}}{2^{g(n)}} = \lim_{n\to\infty} \frac{1}{n} = 0 \neq 1.$$

■

6.042J / 18.062J Mathematics for Computer Science
Spring 2010

Solutions to In-Class Problems Week 9, Wed.

Problem 1.
Recall that for functions f, g on $\mathbb{N}$, $f = O(g)$ iff

$$\exists c \in \mathbb{N}\, \exists n_0 \in \mathbb{N}\, \forall n \geq n_0 \quad c \cdot g(n) \geq |f(n)|\,. \tag{1}$$

For each pair of functions below, determine whether $f = O(g)$ and whether $g = O(f)$. In cases where one function is O() of the other, indicate the *smallest nonegative integer*, c, and for that smallest c, the *smallest corresponding nonegative integer* n_0 ensuring that condition (1) applies.

(a) $f(n) = n^2, g(n) = 3n$.

$f = O(g)$ YES NO If YES, $c =$ _____, n_0 = _____

Solution. NO. ■

$g = O(f)$ YES NO If YES, $c =$ _____, n_0 = _____

Solution. YES, with $c = 1$, $n_0 = 3$, which works because $3^2 = 9$, $3 \cdot 3 = 9$. ■

(b) $f(n) = (3n - 7)/(n + 4), g(n) = 4$

$f = O(g)$ YES NO If YES, $c =$ _____, n_0 = _____

Solution. YES, with $c = 1, n_0 = 0$ (because $|f(n)| < 3$). ■

$g = O(f)$ YES NO If YES, $c =$ _____, n_0 = _____

Solution. YES, with $c = 2, n_0 = 15$.

Since $\lim_{n\to\infty} f(n) = 3$, the smallest possible c is 2. For $c = 2$, the smallest possible $n_0 = 15$ which follows from the requirement that $2f(n_0) \geq 4$. ■

(c) $f(n) = 1 + (n \sin(n\pi/2))^2, g(n) = 3n$

$f = O(g)$ YES NO If yes, $c =$ _____ n_0 = _____

Solution. NO, because $f(2n) = 1$, which rules out $g = O(f)$ since $g = \Theta(n)$. ■

$g = O(f)$ YES NO If yes, $c =$ _____ n_0 = _____

Solution. NO, because $f(2n + 1) = n^2 + 1 \neq O(n)$ which rules out $f = O(g)$. ■

Problem 2.

(a) Define a function $f(n)$ such that $f = \Theta(n^2)$ and $\text{NOT}(f \sim n^2)$.

Solution. Let $f(n) ::= 2n^2$. ■

(b) Define a function $g(n)$ such that $g = O(n^2)$, $g \neq \Theta(n^2)$ and $g \neq o(n^2)$.

Solution. Let $g(n) ::= (n\sin(n\pi/2))^2 + n\,(\cos(n\pi/2))^2$.

For odd n, we have $g(n) = n^2$, which implies that $g \neq o(n^2)$. For even n, we have $g(n) = n$, which implies $n^2 \neq O(g)$ and hence $g \neq \Theta(n^2)$.

■

Problem 3.

False Claim.

$$2^n = O(1). \tag{2}$$

Explain why the claim is false. Then identify and explain the mistake in the following bogus proof.

Bogus proof. The proof by induction on n where the induction hypothesis, $P(n)$, is the assertion (2).

base case: $P(0)$ holds trivially.

inductive step: We may assume $P(n)$, so there is a constant $c > 0$ such that $2^n \leq c \cdot 1$. Therefore,

$$2^{n+1} = 2 \cdot 2^n \leq (2c) \cdot 1,$$

which implies that $2^{n+1} = O(1)$. That is, $P(n+1)$ holds, which completes the proof of the inductive step.

We conclude by induction that $2^n = O(1)$ for all n. That is, the exponential function is bounded by a constant.

■

Solution. A function is $O(1)$ iff it is bounded by a constant, and since the function 2^n grows unboundedly with n, it is not $O(1)$.

The mistake in the bogus proof is in its misinterpretation of the expression 2^n in assertion (2). The intended interpration of (2) is

$$\text{Let } f \text{ be the function defined by the rule } f(n) ::= 2^n. \text{ Then } f = O(1). \tag{3}$$

But the bogus proof treats (2) as an assertion, $P(n)$, about n. Namely, it misinterprets (2) as meaning:

Let f_n be the constant function equal to 2^n. That is, $f_n(k) ::= 2^n$ for all $k \in \mathbb{N}$. Then

$$f_n = O(1). \tag{4}$$

Now (4) is true since every constant function is $O(1)$, and the bogus proof is an unnecessarily complicated, but *correct*, proof that that for each n, the constant function f_n is $O(1)$. But in the last line, the bogus proof switches from the misinterpretation (4) and claims to have proved (3).

So you could say that the exact place where the proof goes wrong is in its first line, where it defines $P(n)$ based on misinterpretation (4). Alternatively, you could say that the proof was a correct proof (of the misinterpretation), and its first mistake was in its last line, when it switches from the misinterpretation to the proper interpretation (3). ■

Problem 4.
Give an elementary proof (without appealing to Stirling's formula) that $\log(n!) = \Theta(n \log n)$.

Solution. One elementary proof goes as follows:

First,

$$\log(n!) = \sum_{i=1}^{n} \log i < \sum_{i=1}^{n} \log n = n \log n.$$

On the other hand,

$$\begin{aligned}
\log(n!) = \sum_{i=1}^{n} \log i &> \sum_{i=\lceil (n+1)/2 \rceil}^{n} \log i \\
&> \sum_{i=\lceil (n+1)/2 \rceil}^{n} \log(n/2) > \frac{n}{2} \cdot \log(n/2) \\
&= \frac{n((\log n) - 1)}{2} = \frac{n \log n}{2} - \frac{n}{2} \\
&> \frac{n \log n}{2} - \frac{n \log n}{6} \qquad \text{for } n > 8. \\
&= \frac{1}{3} \cdot n \log n.
\end{aligned}$$

Therefore, $(1/3)n \log n < \log(n!) < n \log n$ for $n > 8$, proving that $\log(n!) = \Theta(n \log n)$.

■

6.042J / 18.062J Mathematics for Computer Science
Spring 2010

Solutions to In-Class Problems Week 9, Fri.

Problem 1.
A license plate consists of either:

- 3 letters followed by 3 digits (standard plate)
- 5 letters (vanity plate)
- 2 characters – letters or numbers (big shot plate)

Let L be the set of all possible license plates.

(a) Express L in terms of

$$\mathcal{A} = \{A, B, C, \ldots, Z\}$$
$$\mathcal{D} = \{0, 1, 2, \ldots, 9\}$$

using unions ($\cup$) and set products ($\times$).

Solution.

$$L = (A^3 \times D^3) \cup A^5 \cup (A \cup D)^2$$

■

(b) Compute $|L|$, the number of different license plates, using the sum and product rules.

Solution.

$$\begin{aligned}
|L| &= \left|(A^3 \times D^3) \cup A^5 \cup (A \cup D)^2\right| \\
&= \left|(A^3 \times D^3)\right| + \left|A^5\right| + \left|(A \cup D)^2\right| && \text{Sum Rule} \\
&= |A|^3 \cdot |D|^3 + |A|^5 + |A \cup D|^2 && \text{Product Rule} \\
&= |A|^3 \cdot |D|^3 + |A|^5 + (|A| + |D|)^2 && \text{Sum Rule} \\
&= 26^3 \cdot 10^3 + 26^5 + 36^2 = 29458672
\end{aligned}$$

■

Problem 2.
An n-vertex *numbered tree* is a tree whose vertex set is $\{1, 2, \ldots, n\}$ for some $n > 2$. We define the *code* of the numbered tree to be a sequence of $n - 2$ integers from 1 to n obtained by the following recursive process:

> If there are more than two vertices left, write down the *father* of the largest leaf[a], delete this *leaf*, and continue this process on the resulting smaller tree.
>
> If there are only two vertices left, then stop —the code is complete.
>
> [a]The necessarily unique node adjacent to a leaf is called its *father*.

For example, the codes of a couple of numbered trees are shown in the Figure 1.

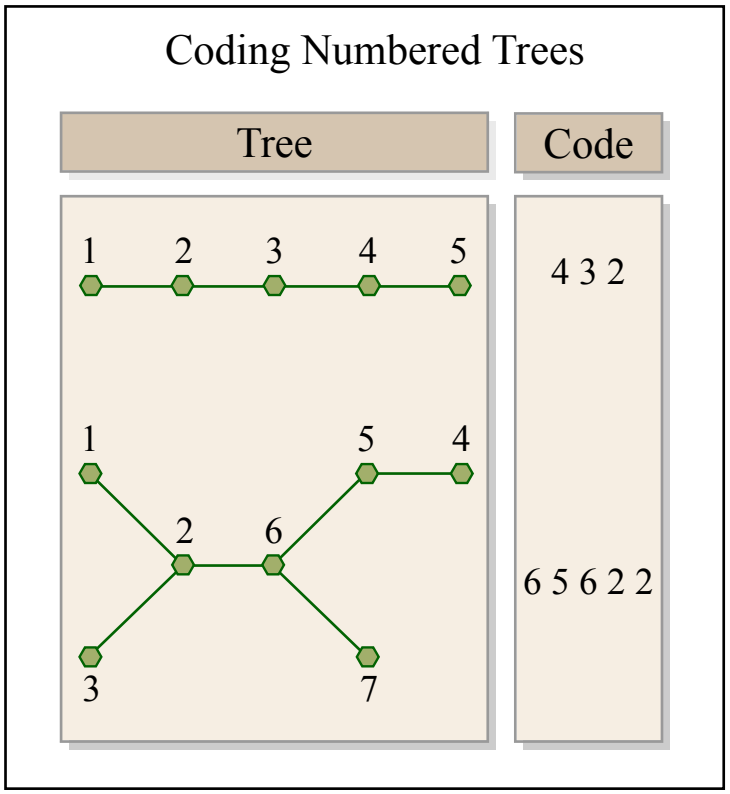


Figure 1:

(a) Describe a procedure for reconstructing a numbered tree from its code.

Solution. The key observation is that, given a code of length $n - 2$, the numbers between 1 and n which *do not appear* in the code are precisely the leaves of the tree. This follows because the vertices left at the end of the process are both leaves. So the procedure must have changed all the nonleaf vertices into leaves, and this implies that all the nonleaf vertices appear in the code.

Hence, the largest missing number is a leaf attached to the first number of the code. The rest of the tree can now be reconstructed by deleting the first number in the code, henceforth ignoring

the largest leaf, and proceeding recursively on the rest of the code. (We're using the obvious fact that what's left after deleting a leaf from a tree is another tree.)

More precisely, the reconstruction procedure applies to any finite tree whose vertex set is totally ordered. The procedure takes *two* parameters: the vertex set, V, and a length $|V| - 2$ "code" sequence, S, of elements in V. If l is the largest element in V which does not appear in S, and f is the first element of S, then the reconstructed tree is obtained by adding edge (l, f) to the tree reconstructed by calling the procedure recursively with first argument $V - \{l\}$ and second argument equal to the code obtained by erasing the initial f from S. The procedure terminates when $|V| = 2$, returning the edge between the two numbers in V.

■

(b) Conclude there is a bijection between the n-vertex numbered trees and $\{1, \ldots, n\}^{n-2}$, and state how many n-vertex numbered trees there are.

Solution. There are exactly as many n-vertex numbered trees as the number of possible code words, that is, the number of length $n - 2$ sequences of integers between 1 and n. So there are n^{n-2} numbered trees.

The reason is that the map from trees to codes is a bijection. To see this, note that the tree reconstruction procedure finds *the only possible tree* with that code. So there can't be two trees with the same code, that is, the map from a tree to its code is an injection. But since the reconstruction procedure finds a tree for every possible codeword, the map from trees to codes is also a surjection. ■

Problem 3. (a) How many of the billion numbers in the range from 1 to 10^9 contain the digit 1? (*Hint:* How many don't?)

Solution. We can count up how many *do not* contain the digit 1 and subtract. So (total number) - (number without 1's) $= 10^9 - (9^9 - 1) = 612,579,512$ (the -1 is for 0 which is not in our range). ■

(b) There are 20 books arranged in a row on a shelf. Describe a bijection between ways of choosing 6 of these books so that no two adjacent books are selected and 15-bit strings with exactly 6 ones.

Solution. A selection of six among twenty books on a shelf corresponds in an obvious way to a 20-bit string with exactly six `1`'s. For example, the 20-bit string with `1`'s in exactly the 3rd, 4th, 5th, 10th, 19th and 20th positions corresponds to selecting 3rd, 4th, 5th, 10th, 19th and 20th books on the shelf.

So the problem reduces to finding a bijection between 20-bit strings with six *nonadjacent* `1`'s and 15-bit strings with six `1`'s.

But in a string, s, with six nonadjacent `1`'s, all but the last `1` must have a `0` to its right. So we can map s to a string with six `1`'s and five fewer `0`'s by erasing the `0`'s immediately to the right of each of the first five `1`'s. For example, erasing the underlined `0`'s in the 20-bit string `0001`$\underline{\texttt{0}}$`1`$\underline{\texttt{0}}$`01`$\underline{\texttt{0}}$`1`$\underline{\texttt{0}}$`000001`$\underline{\texttt{0}}$`10` yields the 15-bit string `000110110000110`.

This map is a bijection because given any 15-bit string with six `1`'s, there is a unique 20-bit string with nonadjacent `1`'s that maps to it, namely, the string obtained by replacing each of the first five `1`'s in the 15-bit string by a `10`. ■

Problem 4.

(a) Let $\mathcal{S}_{n,k}$ be the possible nonnegative integer solutions to the inequality

$$x_1 + x_2 + \cdots + x_k \leq n. \tag{1}$$

That is

$$\mathcal{S}_{n,k} ::= \left\{(x_1, x_2, \ldots, x_k) \in \mathbb{N}^k \mid (1) \text{ is true}\right\}.$$

Describe a bijection between $\mathcal{S}_{n,k}$ and the set of binary strings with n zeroes and k ones.

Solution. The notation $\mathtt{0}^x$ indicates a length x string of `0`'s.

$$(x_1, x_2, \ldots, x_k) \longleftrightarrow \mathtt{0}^{x_1}\mathtt{10}^{x_2}\mathtt{1}\ldots\mathtt{0}^{x_k}\mathtt{10}^{n-s},$$

where $s ::= \sum_{i=1}^{k} x_i$. ■

(b) Let $\mathcal{L}_{n,k}$ be the length k weakly increasing sequences of nonnegative integers $\leq n$. That is

$$\mathcal{L}_{n,k} ::= \left\{(y_1, y_2, \ldots, y_k) \in \mathbb{N}^k \mid y_1 \leq y_2 \leq \cdots \leq y_k \leq n\right\}.$$

Describe a bijection between $\mathcal{L}_{n,k}$ and $\mathcal{S}_{n,k}$.

Solution. $(y_1, y_2, \ldots, y_k) \longleftrightarrow (y_1,\ y_2 - y_1,\ y_3 - y_2,\ \ldots,\ y_k - y_{k-1})$.
In the other direction,

$$(x_1, x_2, \ldots, x_k) \longleftrightarrow (x_1,\ x_1 + x_2,\ x_1 + x_2 + x_3,\ \ldots,\ \sum_{i=1}^{k} x_i).$$

■

6.042J / 18.062J Mathematics for Computer Science
Spring 2010

Solutions to In-Class Problems Week 10, Mon.

Problem 1.
Solve the following problems using the pigeonhole principle. For each problem, try to identify the *pigeons*, the *pigeonholes*, and a *rule* assigning each pigeon to a pigeonhole.

(a) Every MIT ID number starts with a 9 (we think). Suppose that each of the 75 students in 6.042 sums the nine digits of his or her ID number. Explain why two people must arrive at the same sum.

Solution. The students are the pigeons, the possible sums are the pigeonholes, and we map each student to the sum of the digits in his or her MIT ID number. Every sum is in the range from $9 + 8 \cdot 0 = 9$ to $9 + 8 \cdot 9 = 81$, which means that there are 73 pigeonholes. Since there are more pigeons than pigeonholes, there must be two pigeons in the same pigeonhole; in other words, there must be two students with the same sum. ■

(b) In every set of 100 integers, there exist two whose difference is a multiple of 37.

Solution. The pigeons are the 100 integers. The pigeonholes are the numbers 0 to 36. Map integer k to $\text{rem}(k, 37)$. Since there are 100 pigeons and only 37 pigeonholes, two pigeons must go in the same pigeonhole. This means $\text{rem}(k_1, 37) = \text{rem}(k_2, 37,)$, which implies that $k_1 - k_2$ is a multiple of 37. ■

(c) For any five points inside a unit square (not on the boundary), there are two points at distance *less than* $1/\sqrt{2}$.

Solution. The pigeons are the points. The pigeonholes are the four subsquares of the unit square, each of side length $1/2$.

Pigeons are assigned to the subsquare that contains them, except that if the pigeon is on a boundary, it gets assigned to the leftmost and then lowest possible subsquare that includes it (so the point at $(1/2, 1/2)$ is assigned to the lower left subsquare).

There are five pigeons and four pigeonholes, so more than one point must be in the same subsquare. The diagonal of a subsquare is $1/\sqrt{2}$, so two pigeons in the same hole are at most this distance. But pigeons must be inside the unit square, so two pigeons cannot be at the opposite ends of the same subsquare diagonal. So at least one of them must be inside the subsquare, so their distance is less than the length of the diagonal. ■

(d) Show that if $n + 1$ numbers are selected from $\{1, 2, 3, \ldots, 2n\}$, two must be consecutive, that is, equal to k and $k + 1$ for some k.

Solution. The pigeonholes will be the n sets $\{1,2\},\{3,4\},\{5,6\},\ldots,\{2n-1,2n\}$. The pigeons will be the $n+1$ selected numbers. A pigeon is assigned to the unique pigeon hole of which it is a member. By the Pigeonhole Principle, two pigeons must assigned to some hole, and these are the two consecutive numbers required. Notice that we've actually shown a bit more: there will be two consecutive numbers with the smaller being odd. ■

Problem 2.
Answer the following quesions using the Generalized Product Rule.

(a) Next week, I'm going to get really fit! On day 1, I'll exercise for 5 minutes. On each subsequent day, I'll exercise 0, 1, 2, or 3 minutes more than the previous day. For example, the number of minutes that I exercise on the seven days of next week might be 5, 6, 9, 9, 9, 11, 12. How many such sequences are possible?

Solution. The number of minutes on the first day can be selected in 1 way. The number of minutes on each subsequent day can be selected in 4 ways. Therefore, the number of exercise sequences is $1 \cdot 4^6$ by the extended product rule. ■

(b) An *r-permutation* of a set is a sequence of r distinct elements of that set. For example, here are all the 2-permutations of $\{a,b,c,d\}$:

$$\begin{array}{lll} (a,b) & (a,c) & (a,d) \\ (b,a) & (b,c) & (b,d) \\ (c,a) & (c,b) & (c,d) \\ (d,a) & (d,b) & (d,c) \end{array}$$

How many r-permutations of an n-element set are there? Express your answer using factorial notation.

Solution. There are n ways to choose the first element, $n-1$ ways to choose the second, $n-2$ ways to choose the third, ..., and $n-r+1$ ways to choose the r-th element. Thus, there are:

$$n \cdot (n-1) \cdot (n-2) \cdots (n-r+1) = \frac{n!}{(n-r)!}$$

r-permutations of an n-element set. ■

(c) How many $n \times n$ matrices are there with *distinct* entries drawn from $\{1,\ldots,p\}$, where $p \geq n^2$?

Solution. There are p ways to choose the first entry, $p-1$ ways to choose the second for each way of choosing the first, $p-2$ ways of choosing the third, and so forth. In all there are

$$p(p-1)(p-2)\cdots(p-n^2+1) = \frac{p!}{(p-n^2)!}$$

such matrices. Alternatively, this is the number of n^2-permutations of a p element set, which is $p!/(p-n^2)!$. ■

Problem 3.
Your 6.006 tutorial has 12 students, who are supposed to break up into 4 groups of 3 students each. Your TA has observed that the students waste too much time trying to form balanced groups, so he decided to pre-assign students to groups and email the group assignments to his students.

(a) Your TA has a list of the 12 students in front of him, so he divides the list into consecutive groups of 3. For example, if the list is ABCDEFGHIJKL, the TA would define a sequence of four groups to be $(\{A, B, C\}, \{D, E, F\}, \{G, H, I\}, \{J, K, L\})$. This way of forming groups defines a mapping from a list of twelve students to a sequence of four groups. This is a k-to-1 mapping for what k?

Solution. Two lists map to the same sequence of groups iff the first 3 students are the same on both lists, and likewise for the second, third, and fourth consecutive sublists of 3 students. So for a given sequence of 4 groups, the number of lists which map to it is

$$(3!)^4$$

because there are $3!$ ways to order the students in each of the 4 consecutive sublists. ■

(b) A group assignment specifies which students are in the same group, but not any order in which the groups should be listed. If we map a sequence of 4 groups,

$$(\{A, B, C\}, \{D, E, F\}, \{G, H, I\}, \{J, K, L\}),$$

into a group assignment

$$\{\{A, B, C\}, \{D, E, F\}, \{G, H, I\}, \{J, K, L\}\},$$

this mapping is j-to-1 for what j?

Solution. $4!$.

Each of the $4!$ sequences of a particular set of four groups maps to that set of groups. ■

(c) How many group assignments are possible?

Solution.

$$\frac{12!}{4! \cdot (3!)^4} = 15400$$

different assignments.

There are $12!$ possible lists of students, and we can map each list to an assignment by first mapping the list to a sequence of four groups, and then mapping the sequence to the assignment. Since the first map is $(3!)^4$-to-1 and and the second is $4!$-to-1, the composite map is $(3!)^4 \cdot 4!$-to-1. So by the Division Rule, $12! = \left((3!)^4 \cdot 4!\right) A$ where A is the number of assignments. ■

(d) In how many ways can $3n$ students be broken up into n groups of 3?

Solution.

$$\frac{(3n)!}{(3!)^n n!}.$$

This follows simply by replacing "12" by "$3n$" and "4" by "n"in the solution to the previous problem parts. ■

Problem 4.
A pizza house is having a promotional sale. Their commercial reads:

> We offer 9 different toppings for your pizza! Buy 3 large pizzas at the regular price, and you can get each one with as many different toppings as you wish, absolutely free. That's $22,369,621$ different ways to choose your pizzas!

The ad writer was a former Harvard student who had evaluated the formula $(2^9)^3/3!$ on his calculator and gotten close to $22,369,621$. Unfortunately, $(2^9)^3/3!$ is obviously not an integer, so clearly something is wrong. What mistaken reasoning might have led the ad writer to this formula? Explain how to fix the mistake and get a correct formula.

Solution. The number of ways to choose toppings for one pizza is the number of the possible subsets of the set of 9 toppings, namely, 2^9. The ad writer presumably then used the Product Rule to conclude that there were $(2^9)^3$ *sequences* of three topping choices. Then he probably reasoned that each way of making three topping choices arises from 3! sequences, so the Division Rule would imply that the number of ways to choose three pizzas is $(2^9)^3/3!$.

It's true that every set of three *different* topping choices arises from 3! different length-3 sequences of choices. The mistake is that if some of the three choices are the same, then the set of three choices arises from *fewer* than 3! sequences. For example, if all three pizzas have the same toppings, there is only one sequence of topping choices for them.

One fix is to consider ways to choose toppings with 1, 2 and 3 different topping choices. There are $2^9(2^9-1)(2^9-2)/3!$ ways to choose a set of 3 different choices, $2^9(2^9-1)$ ways to choose one topping choice to be used on two pizzas and a second choice for the third pizza, and 2^9 ways to choose one topping for all three pizzas, giving

$$\frac{2^9(2^9-1)(2^9-2)}{3!} + 2^9(2^9-1) + 2^9 = 22,500,864.$$

ways to choose three pizzas.

Alternatively, we can observe that this is exactly the problem of selecting a dozen donuts of five possible different kinds – except now there are 3 donuts and 2^9 kinds. Hence, there is a bijection to the number of (2^9+2)-bit strings with exactly 2^9-1 ones and 3 zeros:

$$\binom{2^9+2}{3} = 22,500,864.$$

■

6.042J / 18.062J Mathematics for Computer Science
Spring 2010

Solutions to In-Class Problems Week 10, Wed.

Problem 1.
The Tao of BOOKKEEPER: we seek enlightenment through contemplation of the word $BOOKKEEPER$.

(a) In how many ways can you arrange the letters in the word $POKE$?

Solution. There are $4!$ arrangements corresponding to the $4!$ permutations of the set $\{P, O, K, E\}$. ■

(b) In how many ways can you arrange the letters in the word BO_1O_2K? Observe that we have subscripted the O's to make them distinct symbols.

Solution. There are $4!$ arrangements corresponding to the $4!$ permutations of the set $\{B, O_1, O_2, K\}$. ■

(c) Suppose we map arrangements of the letters in BO_1O_2K to arrangements of the letters in $BOOK$ by erasing the subscripts. Indicate with arrows how the arrangements on the left are mapped to the arrangements on the right.

$$\begin{array}{ll} O_2BO_1K & \\ KO_2BO_1 & \\ O_1BO_2K & BOOK \\ KO_1BO_2 & OBOK \\ BO_1O_2K & KOBO \\ BO_2O_1K & \ldots \\ \ldots & \end{array}$$

(d) What kind of mapping is this, young grasshopper?

Solution. 2-to-1 ■

(e) In light of the Division Rule, how many arrangements are there of $BOOK$?

Solution. $4!/2$ ■

(f) Very good, young master! How many arrangements are there of the letters in $KE_1E_2PE_3R$?

Solution. $6!$ ■

(g) Suppose we map each arrangement of $KE_1E_2PE_3R$ to an arrangement of $KEEPER$ by erasing subscripts. List all the different arrangements of $KE_1E_2PE_3R$ that are mapped to $REPEEK$ in this way.

Solution. $RE_1PE_2E_3K$, $RE_1PE_3E_2K$, $RE_2PE_1E_3K$, $RE_2PE_3E_1K$, $RE_3PE_1E_2K$, $RE_3PE_2E_1K$ ■

(h) What kind of mapping is this?

Solution. 3!-to-1 ■

(i) So how many arrangements are there of the letters in $KEEPER$?

Solution. $6!/3!$ ■

(j) *Now you are ready to face the BOOKKEEPER!*
How many arrangements of $BO_1O_2K_1K_2E_1E_2PE_3R$ are there?

Solution. $10!$ ■

(k) How many arrangements of $BOOK_1K_2E_1E_2PE_3R$ are there?

Solution. $10!/2!$ ■

(l) How many arrangements of $BOOKKE_1E_2PE_3R$ are there?

Solution. $10!/(2! \cdot 2!)$ ■

(m) How many arrangements of $BOOKKEEPER$ are there?

Solution.

$$\binom{10}{1,2,2,3,1,1} ::= \frac{10!}{1!\ 2!\ 2!\ 3!\ 1!\ 1!} = \frac{10!}{(2!)^2\ 3!}$$

■

Remember well what you have learned: subscripts on, subscripts off.

This is the Tao of Bookkeeper.

(n) How many arrangements of $VOODOODOLL$ are there?

Solution.

$$\binom{10}{1,2,5,2} ::= \frac{10!}{1!\ 2!\ 5!\ 2!}$$

■

(o) How many length 52 sequences of digits contain exactly 17 two's, 23 fives, and 12 nines?

Solution.

$$\binom{52}{17, 23, 12} ::= \frac{52!}{17!\ 23!\ 12!}$$

■

Problem 2. (a) Show that the Magician could not pull off the trick with a deck larger than 124 cards.

Hint: Compare the number of 5-card hands in an n-card deck with the number of 4-card sequences.

Solution. For a match to be possible with a n-card deck, the number, $\binom{n}{5}$, of 5-card hands must be at most as large as the number, $(n)_4$, of 4-card sequences. So

$$(n)_4(n-4)/5! = \binom{n}{5} \leq (n)_4,$$

which implies

$$n - 4 \leq 5!$$

and hence $n \leq 124$.

■

(b) Show that, in principle, the Magician could pull off the Card Trick with a deck of 124 cards.

Hint: Hall's Theorem and degree-constrained (10.6.5) graphs.

Solution. In principle the trick is possible iff the bipartite graph between 5-card hands and 4-card sequences has a matching for the hands. In this graph, the degree of each hand is $5! = 120$, whatever the size of deck. The degree of each sequence of 4 will be the number of cards remaining in the deck. With a deck of 124, there will be 120 cards remaining, so the degree of each sequence of 4 will also be 120. Hence, the graph is degree-constrained, and so satisfies Hall's condition for a matching. ■

Problem 3.
The Magician can determine the 5th card in a poker hand when his Assisant reveals the other 4 cards. Describe a similar method for determining 2 hidden cards in a hand of 9 cards when your Assisant reveals the other 7 cards.

Solution. Since there must be $\lceil 9/4 \rceil = 3$ cards with the same suit, our collaborator chooses to hide two of them and then use the third one as the first card to be revealed. So this first revealed card fixes the suit of the two hidden cards; it will also be used as the origin for the offset position of the first hidden card. This first hidden card will in turn be used as the origin for the offset of the other hidden card. There are six cards to code the two offset positions. These suffice to code two offsets of size from one to six. That is, our collaborator can choose one of the $3! = 6$ orders in which to reveal the first three cards and thereby tell us the offset position of the first hidden card. Our collaborator can then choose the order of the final three cards to describe the offset position of the second hidden card from the first. Note that the first revealed card must be chosen so that

both offsets are ≤ 6; since the sum of the offsets between successive cards ordered in a cycle from Ace to King is 13, it is not possible for more than one offset between successive cards to exceed seven, so this is always possible.

■

Problem 4.
Solve the following counting problems. Define an appropriate mapping (bijective or k-to-1) between a set whose size you know and the set in question.

(a) An independent living group is hosting nine new candidates for membership. Each candidate must be assigned a task: 1 must wash pots, 2 must clean the kitchen, 3 must clean the bathrooms, 1 must clean the common area, and 2 must serve dinner. Write a multinomial coefficient for the number of ways this can be done.

Solution. There is a bijection from sequences containing one P, two K's, three B's, a C, and two D's. In any such sequence, the letter in the ith position specifies the task assigned to the ith candidate. Therefore, the number of possible assignments is:

$$\binom{9}{1,2,3,1,2} ::= \frac{9!}{1!\,2!\,3!\,1!\,2!}$$

■

(b) Write a multinomial coefficient for the number of nonnegative integer solutions for the equation:

$$x_1 + x_2 + x_3 + x_4 + x_5 = 8. \tag{1}$$

Solution. There is a bijection from solutions over $\mathbb{N}$ for (1) to bit strings with eight 0's and four 1's. Namely, letting 0^x represent a string of x zeroes,

$$(x_1, x_2, x_3, x_4, x_5) \in \mathbb{N}^5 \mapsto 0^{x_1}10^{x_2}10^{x_3}10^{x_4}10^{x_5}$$

Therefore, there are

$$\binom{12}{4}$$

nonnegative integer solutions to (1). ■

(c) How many nonnegative integers less than 1,000,000 have exactly one digit equal to 9 and have a sum of digits equal to 17?

Solution. We identify the nonnegative integers less than 1,000,000 with the length 6 strings of decimal digits. Then there is a bijection with pairs:

$$(\text{position of the } 9, \text{successive values of other 5 digits})$$

The sum of the other 5 digits is equal to 8, so the number of ways to choose their values is equal to the number of solutions over the nonnegative integers to (1), namely, $\binom{12}{4}$. So by the product rule there are

$$6 \cdot \binom{12}{4}$$

such integers. ■

6.042J / 18.062J Mathematics for Computer Science
Spring 2010

Solutions to In-Class Problems Week 10, Fri.

Problem 1.
A certain company wants to have security for their computer systems. So they have given everyone a name and password. A length 10 word containing each of the characters:

a, d, e, f, i, l, o, p, r, s,

is called a *cword*. A password will be a cword which does not contain any of the subwords "fails", "failed", or "drop".

For example, the following two words are passwords:

adefiloprs, srpolifeda,

but the following three cwords are not:

a**drop**eflis, **failedrop**s, **drop**e**fails**.

(a) How many cwords contain the subword "drop"?

Solution. Such cwords are obtainable by taking the word "drop" and the remaining 6 letters in any order. There are 7! permutations of these 7 items. ■

(b) How many cwords contain both "drop" and "fails"?

Solution. Take the words "drop" and "fails" and the remaining letter "e" in any order. So there are 3! such cwords.

■

(c) Use the Inclusion-Exclusion Principle to find a simple formula for the number of passwords.

Solution. There are 7! cwords that contain "drop", 6! that contain "fails", and 5! that contain "failed". There are 3! cwords containing both "drop" and "fails". No cword can contain both "fails" and "failed". The cwords containing both "drop" and "failed" come from taking the subword "failedrop" and the remaining letter "s" in any order, so there are 2! of them. So by Inclusion-exclusion, we have the number of cwords containing at least one of the three forbidden subwords is

$$(7! + 6! + 5!) - (3! + 0 + 2!) + 0 = 5!(49) - 8.$$

Among the 10! cwords, the remaining ones are passwords, so the number of passwords is

$$10! - 7! - 6! - 5! + 3! + 2! = 3,622,928.$$

■

Problem 2.
Solve the following counting problems by defining an appropriate mapping (bijective or k-to-1) between a set whose size you know and the set in question.

(a) How many different ways are there to select a dozen donuts if four varieties are available?

Solution. There is a bijection from selections of a dozen donuts to 15-bit sequences with exactly 3 ones. In particular, suppose that the varieties are glazed, chocolate, lemon, and Boston creme. Then a selection of g glazed, c chocolate, l lemon, and b Boston creme maps to the sequence:

$$(g\ 0's)\ 1\ (c\ 0's)\ 1\ (l\ 0's)\ 1\ (b\ 0's)$$

Therefore, the number of selections is equal to the number of 15-bit sequences with exactly 3 ones, which is:

$$\frac{15!}{3!\ 12!} = \binom{15}{3}$$

■

(b) In how many ways can Mr. and Mrs. Grumperson distribute 13 identical pieces of coal to their two —no, three! —children for Christmas?

Solution. There is a bijection from 15-bit strings with two ones. In particular, the bit string $0^a10^b10^c$ maps to the assignment of a coals to the first child, b coals to the second, and c coals to the third. Therefore, there are $\binom{15}{2}$ assignments. ■

(c) How many solutions over the nonnegative integers are there to the inequality:

$$x_1 + x_2 + \ldots + x_{10} \quad \leq \quad 100$$

Solution. There is a bijection from 110-bit sequences with 10 ones to solutions to this equation. In particular, x_i is the number of zeros before the i-th one but after the $(i-1)$-st one (or the beginning of the sequence). Therefore, there are $\binom{110}{10}$ solutions. ■

(d) We want to count step-by-step paths between points in the plane with integer coordinates. Ony two kinds of step are allowed: a right-step which increments the x coordinate, and an up-step which increments the y coordinate.

(i) How many paths are there from $(0, 0)$ to $(20, 30)$?

Solution. $\binom{50}{20}$.
There is a bijection from 50-bit sequences with 20 zeros and 30 ones. The sequence $(b_1, \ldots, b_{30})$ maps to a path where the i-th step is right if $b_i = 0$ and up if $b_i = 1$. Therefore, the number of paths is equal to $\binom{50}{20}$. ■

(ii) How many paths are there from $(0, 0)$ to $(20, 30)$ that go through the point $(10, 10)$?

Solution. $\binom{20}{10} \cdot \binom{30}{10}$.
There is a bijection between the paths from $(20, 30)$ that go through $(10, 10)$ and set of pairs of paths consisting of path from $(0, 0)$ to $(10, 10)$ and a path from $(10, 10)$ to $(20, 30)$. So the number of paths through $(10, 10)$ is the product of the sizes of these two sets of paths. ■

(iii) How many paths are there from $(0, 0)$ to $(20, 30)$ that do *not* go through either of the points $(10, 10)$ and $(15, 20)$?
Hint: Let P be the set of paths from $(0, 0)$ to $(20, 30)$, N_1 be the paths in P that go through $(10, 10)$ and N_2 be the paths in P that go through $(15, 20)$.

Solution.

$$\binom{50}{20} - \binom{20}{10} \cdot \binom{30}{10} - \binom{30}{15} \cdot \binom{15}{5} + \binom{20}{10} \cdot \binom{15}{5} \cdot \binom{15}{5}.$$

$N_1 \cap N_2$ is the set of paths from $(0, 0)$ to $(20, 30)$ that go through both $(10, 10)$ and $(15, 20)$. So $P - (N_1 \cup N_2)$ is the set of paths to be counted. Now we have

$$\begin{aligned} |P - (N_1 \cup N_2)| &= |P| - |N_1 \cup N_2| \\ &= |P| - |N_1| - |N_2| + |N_1 \cap N_2| \qquad \text{by Inclusion-Exclusion.} \end{aligned}$$

Part (ii) shows how to calculate $|N_i|$. Also, there is a bijection between $N_1 \cap N_2$ and the set of triples consisting of a path $(0, 0)$ to $(10, 10)$, a path from $(10, 10)$ to $(15, 20)$, and a path from $(15, 20)$ to $(20, 30)$. So the size of $N_1 \cap N_2$ is the product of the sizes of these three sets of paths.

■

Problem 3.
Here are the solutions to the next 10 problem parts, in no particular order.

$$n^m \qquad m^n \qquad \frac{n!}{(n-m)!} \qquad \binom{n+m}{m} \qquad \binom{n-1+m}{m} \qquad \binom{n-1+m}{n} \qquad 2^{mn}$$

(a) How many solutions over the natural numbers are there to the inequality $x_1 + x_2 + \cdots + x_n \leq m$? _____

Solution.

$$\binom{n+m}{m}$$

This is the same as the number of solutions to the equation the equality $x_1 + x_2 + \cdots + x_n + y = m$, and which has a bijection to sequences with m stars and n bars. ■

(b) How many length m words can be formed from an n-letter alphabet, if no letter is used more than once? _____

Solution.

$$\frac{n!}{(n-m)!}$$

There are n choices for the first letter, $n-1$ choices for the second letter, $\ldots n-m+1$ choices for the mth letter, so by the Generalized Product rule, the number of words is

$$n \cdot (n-1) \cdots (n-m+1).$$

■

(c) How many length m words can be formed from an n-letter alphabet, if letters can be reused? _____

Solution. n^m by the Product Rule. ■

(d) How many binary relations are there from set A to set B when $|A| = m$ and $|B| = n$? _____

Solution.

$$2^{mn}$$

The graph of a binary relations from A to B is a subset of $A \times B$. There are on 2^{mn} such subsets because $|A \times B| = mn$. ■

(e) How many injections are there from set A to set B, where $|A| = m$ and $|B| = n \geq m$? _____

Solution.

$$\frac{n!}{(n-m)!}$$

There is a bijection between the injections and the length m sequences of distinct elements of B. By the Generalized Product rule, the number of such sequences is

$$n \cdot (n-1) \cdots (n-m+1).$$

■

(f) How many ways are there to place a total of m distinguishable balls into n distinguishable urns, with some urns possibly empty or with several balls? _____

Solution.

$$n^m$$

There is a bijection between a placement of the balls and length m sequence whose ith element is the urn where the ith ball is placed. So the number of placements is the same as the number of length m sequences of elements from a size-n set. ■

(g) How many ways are there to place a total of m indistinguishable balls into n distinguishable urns, with some urns possibly empty or with several balls? _____

Solution.

$$\binom{n-1+m}{m}$$

This is the same as the number of selections of m donuts with n possible flavors, which is the number of sequences with m stars and $n-1$ bars. ■

(h) How many ways are there to put a total of m distinguishable balls into n distinguishable urns with at most one ball in each urn? _____

Solution.

$$\frac{n!}{(n-m)!}$$

There is a bijection between a placement of balls and a length m sequence whose ith element is the urn containing the ith ball. So the number of ball placements is the same as number of length m sequences of distinct elements from a set of n elements. ■

6.042J / 18.062J Mathematics for Computer Science
Spring 2010

Solutions to In-Class Problems Week 11, Wed.

Problem 1.
Find the coefficients of

(a) x^5 in $(1+x)^{11}$

Solution.

$$\binom{11}{5} = 462$$

■

(b) x^8y^9 in $(3x+2y)^{17}$

Solution.

$$\binom{17}{8}3^8 2^9.$$

When $(3x+2y)^{17}$ is expressed as a sum of powers of the summands $3x$ and $2y$, the coefficient of $(3x)^8(2y)^9$ is $\binom{17}{8}$, so the coefficient of x^8y^9 is this binomial coefficient times $3^8 \cdot 2^9$. ■

(c) a^6b^6 in $(a^2+b^3)^5$

Solution. $a^6b^6 = (a^2)^3(b^3)^2$, so the coefficient is

$$\binom{5}{3} = 10$$

■

Problem 2.
You want to choose a team of m people for your startup company from a pool of n applicants, and from these m people you want to choose k to be the team managers. You took 6.042, so you know you can do this in

$$\binom{n}{m}\binom{m}{k}$$

ways. But your CFO, who went to Harvard Business School, comes up with the formula

$$\binom{n}{k}\binom{n-k}{m-k}.$$

Before doing the reasonable thing —dump on your CFO or Harvard Business School —you decide to check his answer against yours.

(a) Give a *combinatorial proof* that your CFO's formula agrees with yours.

Solution. Instead of choosing first m from n and then k from the chosen m, you could alternately choose the k managers from the n people and then choose $m-k$ people to fill out the team from the remaining $n-k$ people. This gives you $\binom{n}{k}\binom{n-k}{m-k}$ ways of picking your team. Since you must have the same number of options regardless of the order in which you choose to pick team members and managers,

$$\binom{n}{m}\binom{m}{k} = \binom{n}{k}\binom{n-k}{m-k}.$$

Formally, in the first method we count the number of pairs (A, B), where A is a size m subset of the pool of n applicants, and B is a size k subset of A. By the Generalized Product Rule, there are

$$\binom{n}{m} \cdot \binom{m}{k}$$

such pairs.

In the second method, we count pairs (C, D), where C is a size k subset of the applicant pool, and D is a size $(m-k)$ subset of the pool that is disjoint from C. By the Generalized Product Rule, there are

$$\binom{n}{k} \cdot \binom{n-k}{m-k}$$

such pairs.

These two expressions are equal because there is an obvious bijection between the two kinds of pairs, namely map (A, B) to $(B, A-B)$. ■

(b) Verify this combinatorial proof by giving an *algebraic* proof of this same fact.

Solution.

$$\begin{aligned}
\binom{n}{m}\binom{m}{k} &= \frac{n!}{m!(n-m)!}\frac{m!}{k!(m-k)!} \\
&= \frac{n!}{(n-m)!k!(m-k)!} \\
&= \frac{n!(n-k)!}{(n-m)!k!(m-k)!(n-k)!} \\
&= \frac{n!}{k!(n-k)!}\frac{(n-k)!}{(n-m)!(m-k)!} \\
&= \frac{n!}{k!(n-k)!}\frac{(n-k)!}{((n-k)-(m-k))!(m-k)!} \\
&= \binom{n}{k}\binom{n-k}{m-k}.
\end{aligned}$$

■

Problem 3. (a) Now give a combinatorial proof of the following, more interesting theorem:

$$n2^{n-1} = \sum_{k=1}^{n} k\binom{n}{k} \tag{1}$$

Hint: Let S be the set of all length-n sequences of 0's, 1's and a single *.

Solution. Let $P ::= \{0, \ldots, n-1\} \times \{0,1\}^{n-1}$. On the one hand, there is a bijection from P to S by mapping (k, x) to the word obtained by inserting a * just after the kth bit in the length-$n-1$ binary word, x. So

$$|S| = |P| = n2^{n-1} \tag{2}$$

by the Product Rule.

On the other hand, every sequence in S contains between 1 and n nonzero entries since the $*$, at least, is nonzero. The mapping from a sequence in S with exactly k nonzero entries to a pair consisting of the set of positions of the nonzero entries and the position of the * among these entries is a bijection, and the number of such pairs is $\binom{n}{k}k$ by the Generalized Product Rule. Thus, by the Sum Rule:

$$|S| = \sum_{k=1}^{n} k\binom{n}{k}$$

Equating this expression and the expression (2) for $|S|$ proves the theorem. ■

(b) Now prove (1) algebraically by applying the Binomial Theorem to $(1+x)^n$ and taking derivatives.

Solution. By the Binomial Theorem

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k.$$

Taking derivatives, we get

$$\begin{aligned} n(1+x)^{n-1} &= \sum_{k=0}^{n} k\binom{n}{k} x^{k-1} \\ &= \frac{1}{x}\sum_{k=0}^{n} k\binom{n}{k} x^k. \end{aligned} \tag{3}$$

Letting $x = 1$ in (3) yields (1).

■

6.042J / 18.062J Mathematics for Computer Science
Spring 2010

Solutions to In-Class Problems Week 11, Fri.

Problem 1.
We are interested in generating functions for the number of different ways to compose a bag of n donuts subject to various restrictions. For each of the restrictions in (a)-(e) below, find a closed form for the corresponding generating function.

(a) All the donuts are chocolate and there are at least 3.

Solution.

$$\langle 0,0,0,1,1,\ldots,1,\ldots\rangle \longleftrightarrow \frac{x^3}{1-x}$$

■

(b) All the donuts are glazed and there are at most 2.

Solution.

$$\langle 1,1,1,0,0,\ldots,0,\ldots\rangle \longleftrightarrow 1+x+x^2$$

■

(c) All the donuts are coconut and there are exactly 2 or there are none.

Solution.

$$\langle 1,0,1,0,0,\ldots,0,\ldots\rangle \longleftrightarrow 1+x^2$$

■

(d) All the donuts are plain and their number is a multiple of 4.

Solution.

$$\langle 1,0,0,0,1,0,0,0,\ldots,1,0,0,0,\ldots\rangle \longleftrightarrow \frac{1}{1-x^4}$$

■

(e) The donuts must be chocolate, glazed, coconut, or plain and:

- there must be at least 3 chocolate donuts, and
- there must be at most 2 glazed, and
- there must be exactly 0 or 2 coconut, and
- there must be a multiple of 4 plain.

Solution.

$$\frac{x^3}{1-x}(1+x+x^2)(1+x^2)\frac{1}{1-x^4} = \frac{x^3(1+x+x^2)(1+x^2)}{(1-x)^2(1+x)(1+x^2)}$$
$$= x^3\frac{1+x+x^2}{(1-x)^2(1+x)}$$

■

(f) Find a closed form for the number of ways to select n donuts subject to the constraints of the previous part.

Solution. Let

$$G(x) ::= \frac{1+x+x^2}{(1-x)^2(1+x)},$$

so the generating function for donut selections is $x^3G(x)$. By partial fractions

$$\frac{1+x+x^2}{(1-x)^2(1+x)} = \frac{A}{1-x} + \frac{B}{(1-x)^2} + \frac{C}{1+x} \tag{1}$$

for some constants, A, B, C. We know that the coefficient of x^n in the series for $(1-x)^2$ is, by the Convolution Rule, the number of ways to select n items of two different kinds, namely, $\binom{n+1}{1} = n+1$, so we conclude that the nth coefficient in the series for $G(x)$ is

$$A + B(n+1) + C(-1)^n. \tag{2}$$

To find A, B, C, we multiply both sides of (1) by the denominator $(1-x)^2(1+x)$ to obtain

$$1+x+x^2 = A(1-x)(1+x) + B(1+x) + C(1-x)^2. \tag{3}$$

Letting $x = 1$ in (3), we conclude that $3 = 2B$, so $B = 3/2$. Then, letting $x = -1$, we conclude $(-1)^2 = C2^2$, so $C = 1/4$. Finally, letting $x = 0$, we have

$$1 = A + B + C = A + \frac{3}{2} + \frac{1}{4},$$

so $A = -3/4$. Then from (2), we conclude that the nth coefficient in the series for $G(x)$ is

$$-\frac{3}{4} + \frac{3(n+1)}{2} + \frac{(-1)^n}{4} = \frac{6n+3+(-1)^n}{4}.$$

So the nth coefficient in the series for the generating function, $x^3G(x)$, for donut selections is zero for $n < 3$, and, for $n \geq 3$, is the $(n-3)$rd coefficient of G, namely,

$$\frac{6(n-3)+3+(-1)^{n-3}}{4} = \frac{6n-15+(-1)^{n-1}}{4}.$$

■

Problem 2. (a) Let

$$S(x) ::= \frac{x^2 + x}{(1-x)^3}.$$

What is the coefficient of x^n in the generating function series for $S(x)$?

Solution. n^2. That is, $S(x) = \sum_{n=1}^{\infty} n^2 x^n$.

To see why, note that the coefficient of x^n in $1/(1-x)^3$ is, by the Convolution Rule, the number of ways to select n items of three different kinds, namely,

$$\binom{n+2}{2} = \frac{(n+2)(n+1)}{2}.$$

Now the coefficient of x^n in $x^2/(1-x)^3$ is the same as the coefficient of x^{n-2} in $1/(1-x)^3$, namely, $((n-2)+2)((n-2)+1)/2 = n(n-1)/2$. Similarly, the coefficient of x^n in $x/(1-x)^3$ is the same as the coefficient of x^{n-1} in $1/(1-x)^3$, namely, $((n-1)+2)((n-1)+1)/2 = (n+1)n/2$. The coefficient of x^n in $S(x)$ is the sum of these two coefficients, namely,

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

■

(b) Explain why $S(x)/(1-x)$ is the generating function for the sums of squares. That is, the coefficient of x^n in the series for $S(x)/(1-x)$ is $\sum_{k=1}^{n} k^2$.

Solution.

$$\left(\sum_{n=0}^{\infty} a_n x^n\right)\left(\sum_{n=0}^{\infty} x^n\right) = \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n} a_k \cdot 1\right)x^n = \sum_{n=0}^{\infty}\left(\sum_{k=0}^{n} a_k\right)x^n \tag{4}$$

by the convolution formula for the product of series. For $S(x)$, the coefficient of x^k is $a_k = k^2$, and

$$S(x)/(1-x) = S(x)\left(\sum_{n=0}^{\infty} x^n\right),$$

so (4) implies that the coefficient of x^n in $S(x)/(1-x)$ is the sum of the first n squares. ■

(c) Use the previous parts to prove that

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

Solution. We have

$$\frac{S(x)}{1-x} = \frac{\left(\frac{x(1+x)}{(1-x)^3}\right)}{1-x} = \frac{x+x^2}{(1-x)^4}. \tag{5}$$

The coefficient of x^n in the series expansion of $1/(1-x)^4$ is

$$\binom{n+3}{3} = \frac{(n+1)(n+2)(n+3)}{3!}.$$

But by (5),

$$\frac{S(x)}{1-x} = \frac{x}{(1-x)^4} + \frac{x^2}{(1-x)^4},$$

so the coefficient of x^n is the sum of the $(n-1)$st and $(n-2)$nd coefficients of $(1-x)^4$, namely,

$$\frac{n(n+1)(n+2)}{3!} + \frac{(n-1)n(n+1)}{3!} = \frac{n(n+1)(2n+1)}{6}.$$

■

Appendix

Let $[x^n]F(x)$ denote the coefficient of x^n in the power series for $F(x)$. Then,

$$[x^n]\left(\frac{1}{(1-\alpha x)^k}\right) = \binom{n+k-1}{k-1}\alpha^n. \tag{6}$$

Partial Fractions

Here's a particular case of the Partial Fraction Rule that should be enough to illustrate the general Rule. Let

$$r(x) ::= \frac{p(x)}{(1-\alpha x)^2(1-\beta x)(1-\gamma x)^3}$$

where α, β, γ are distinct complex numbers, and $p(x)$ is a polynomial of degree less than the demoninator, namely, less than 6. Then there are unique numbers $a_1, a_2, b, c_1, c_2, c_3 \in \mathbb{C}$ such that

$$r(x) = \frac{a_1}{1-\alpha x} + \frac{a_2}{(1-\alpha x)^2} + \frac{b}{1-\beta x} + \frac{c_1}{1-\gamma x} + \frac{c_2}{(1-\gamma x)^2} + \frac{c_3}{(1-\gamma x)^3}$$

6.042J / 18.062J Mathematics for Computer Science
Spring 2010

Solutions to In-Class Problems Week 12, Mon.

Problem 1.
The famous mathematician, Fibonacci, has decided to start a rabbit farm to fill up his time while he's not making new sequences to torment future college students. Fibonacci starts his farm on month zero (being a mathematician), and at the start of month one he receives his first pair of rabbits. Each pair of rabbits takes a month to mature, and after that breeds to produce one new pair of rabbits each month. Fibonacci decides that in order never to run out of rabbits or money, every time a batch of new rabbits is born, he'll sell a number of newborn pairs equal to the total number of pairs he had three months earlier. Fibonacci is convinced that this way he'll never run out of stock.

(a) Define the number, r_n, of pairs of rabbits Fibonacci has in month n, using a recurrence relation. That is, define r_n in terms of various r_i where $i < n$.

Solution. According to the description above, $r_0 = 0$ and $r_1 = 1$. Since the rabbit pair received at the first month is too young to breed, $r_2 = 1$ as well. After that, r_n is equal to the number, r_{n-1}, of rabbit pairs in the previous month, plus the number of newborn pairs, minus the number, r_{n-3}, he sells. The number of newborn pairs equals to the number of breeding pairs from the previous month, which is precisely the total number, r_{n-2}, of pairs from two months before.

Thus,

$$r_n = r_{n-1} + (r_{n-2} - r_{n-3}).$$

■

(b) Let $R(x)$ be the generating function for rabbit pairs,

$$R(x) ::= r_0 + r_1 x + r_2 x^2 + \cdot.$$

Express $R(x)$ as a quotient of polynomials.

Solution. Reasoning as in the derivation of the generating function for the orginal Fibonacci numbers, we have

$$\begin{array}{rcccccccccc}
R(x) & = & r_0 & + & r_1 x & + & r_2 x^2 & + & r_3 x^3 & + & r_4 x^4 + \cdots. \\
-xR(x) & = & & - & r_0 x & - & r_1 x^2 & - & r_2 x^3 & - & r_3 x^4 - \cdots. \\
-x^2 R(x) & = & & & & - & r_0 x^2 & - & r_1 x^3 & - & r_2 x^4 - \cdots. \\
x^3 R(x) & = & & & & & & + & r_0 x^3 & + & r_1 x^4 + \cdots. \\
\hline
R(x)(1 - x - x^2 + x^3) & = & r_0 & + & (r_1 - r_0)x & + & (r_2 - r_1 - r_0)x^2 & + & 0x^3 & + & 0x^4 + \cdots. \\
& = & 0 & + & 1x & + & 0x^2. & & & &
\end{array}$$

so

$$R(x) = \frac{x}{1 - x - x^2 + x^3} = \frac{x}{(1+x)(1-x)^2}\,. \tag{1}$$

■

(c) Find a partial fraction decomposition of the generating function $R(x)$.

Solution. We know

$$R(x) = \frac{A}{1+x} + \frac{B}{1-x} + \frac{C}{(1-x)^2}$$

for some numbers A, B, C. Multiplying both sides of this equation by $(1+x)(1-x)^2$ gives

$$x = A(1-x)^2 + B(1+x)(1-x) + C(1+x).$$

Letting $x = 1$ gives $C = 1/2$, letting $x = -1$ gives $A = -1/4$, and letting $x = 0$ then gives $B = -(A + C) = -1/4$. ■

(d) Finally, use the partial fraction decomposition to come up with a closed form expression for the number of pairs of rabbits Fibonacci has on his farm on month n.

Solution. We find the coefficient as the sum of the coefficients for each term in the partial fraction expansion.

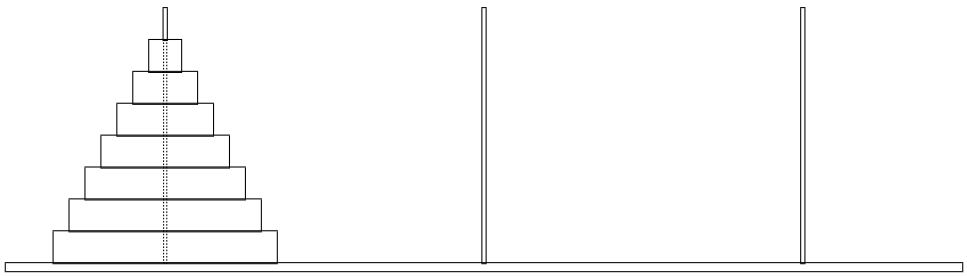
$$\begin{array}{rcccccccccc}
A/(1+x) & = & - & 1/4 & - & (1/4)(-x) & - & (1/4)(-x)^2 & - & \cdots & - & (1/4)(-x)^n - \cdots \\
B/(1-x) & = & - & 1/4 & - & (1/4)x & - & (1/4)x^2 & - & \cdots & - & (1/4)x^n - \cdots \\
C/(1-x)^2 & = & & 1/2 & + & (2/2)x & + & (3/2)x^2 & + & \cdots & + & ((n+1)/2)x^n + \cdots \\
\hline
R(x) & = & & & & 1x & + & 1x^2 & + & \cdots & + & \left(\frac{n+1}{2} - \frac{(-1)^n+1}{4}\right)x^n + \cdots
\end{array}$$

so

$$r_n = \left\lceil \frac{n}{2} \right\rceil\,.$$

■

Problem 2.
Less well-known than the Towers of Hanoi —but no less fascinating —are the Towers of Sheboygan. As in Hanoi, the puzzle in Sheboygan involves 3 posts and n disks of different sizes. Initially, all the disks are on post #1:



The objective is to transfer all n disks to post #2 via a sequence of moves. A move consists of removing the top disk from one post and dropping it onto another post with the restriction that a larger disk can never lie above a smaller disk. Furthermore, a local ordinance requires that *a disk can be moved only from a post to the next post on its right —or from post #3 to post #1.* Thus, for example, moving a disk directly from post #1 to post #3 is not permitted.

(a) One procedure that solves the Sheboygan puzzle is defined recursively: to move an initial stack of n disks to the next post, move the top stack of $n-1$ disks to the furthest post by moving it to the next post two times, then move the big, nth disk to the next post, and finally move the top stack another two times to land on top of the big disk. Let s_n be the number of moves that this procedure uses. Write a simple linear recurrence for s_n.

Solution.

$$\begin{aligned} &s_0 = 0, \\ &s_n = 2s_{n-1} + 1 + 2s_{n-1} = 4s_{n-1} + 1 \qquad \text{for } n > 0. \end{aligned} \tag{2}$$

■

(b) Let $S(x)$ be the generating function for the sequence $\langle s_0, s_1, s_2, \ldots \rangle$. Show that $S(x)$ is a quotient of polynomials.

Solution.

$$\begin{array}{rcrcrcrcr} S(x) & = & s_0 & + & s_1 x & + & s_2 x^2 & + & s_3 x^3 + \cdots . \\ -4xS(x) & = & & - & 4s_0 x & - & 4s_1 x^2 & - & 4s_2 x^3 - \cdots . \\ -1/(1-x) & = & -1 & - & 1x & - & 1x^2 & - & 1x^3 - \cdots . \\ \hline S(x)(1-4x) - \frac{1}{1-x} & = & -1 & + & 0x & + & 0x^2 & + & 0x^3 + \cdots . \\ & = & -1. & & & & & & \end{array}$$

so

$$S(x)(1-4x) - \frac{1}{1-x} = -1,$$

and

$$S(x) = \frac{x}{(1-x)(1-4x)}\,.$$

■

(c) Give a simple formula for s_n.

Solution. We can express $x/(1-x)(1-4x)$ using partial fractions as

$$\frac{x}{(1-x)(1-4x)} = \frac{a}{1-x} + \frac{b}{1-4x} \tag{3}$$

for some constants a, b. Multiplying both sides of (3) by the left hand denominator yields

$$x = a(1-4x) + b(1-x). \tag{4}$$

Letting $x = 1$ yields $a = -1/3$ and letting $x = 1/4$ yields $b = 1/3$. Now from (3), we have

$$S(x) = \frac{-1/3}{1-x} + \frac{1/3}{1-4x}$$

so

$$s_n = -\frac{1}{3} + \frac{1}{3}4^n = \frac{4^n - 1}{3}.$$

■

(d) A better (indeed optimal, but we won't prove this) procedure to solve the Towers of Sheboygan puzzle can be defined in terms of two mutually recursive procedures, procedure $P_1(n)$ for moving a stack of n disks 1 pole forward, and $P_2(n)$ for moving a stack of n disks 2 poles forward. This is trivial for $n = 0$. For $n > 0$, define:

$P_1(n)$: Apply $P_2(n-1)$ to move the top $n-1$ disks two poles forward to the third pole. Then move the remaining big disk once to land on the second pole. Then apply $P_2(n-1)$ again to move the stack of $n-1$ disks two poles forward from the third pole to land on top of the big disk.

$P_2(n)$: Apply $P_2(n-1)$ to move the top $n-1$ disks two poles forward to land on the third pole. Then move the remaining big disk to the second pole. Then apply $P_1(n-1)$ to move the stack of $n-1$ disks one pole forward to land on the first pole. Now move the big disk 1 pole forward again to land on the third pole. Finally, apply $P_2(n-1)$ again to move the stack of $n-1$ disks two poles forward to land on the big disk.

Let t_n be the number of moves needed to solve the Sheboygan puzzle using procedure $P_1(n)$. Show that

$$t_n = 2t_{n-1} + 2t_{n-2} + 3, \tag{5}$$

for $n > 1$.

Hint: Let s_n be the number of moves used by procedure $P_2(n)$. Express each of t_n and s_n as linear combinations of t_{n-1} and s_{n-1} and solve for t_n.

Solution. From the definitions of procedures P_1 and P_2 we have

$$\begin{aligned}
t_0 &= 0, \\
s_0 &= 0, \\
t_n &= s_{n-1} + 1 + s_{n-1} && \text{for } n > 0, && (6)\\
s_n &= s_{n-1} + 1 + t_{n-1} + 1 + s_{n-1} && \text{for } n > 0. && (7)
\end{aligned}$$

Using (6) to get $s_{n-1} = (t_n - 1)/2$ and then expressing s's in (7) in terms of t's, we conclude that for $n > 0$,

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

so

$$t_{n+1} = 2t_n + 2t_{n-1} + 3,$$

which is the same as the given recurrence (5) with $n + 1$ replacing n. ■

(e) Derive values a, b, c, α, β such that

$$t_n = a\alpha^n + b\beta^n + c.$$

Conclude that $t_n = o(s_n)$.

Solution.

$$t_n = \frac{(1+\sqrt{3})^n}{3-\sqrt{3}} + \frac{(1-\sqrt{3})^n}{3+\sqrt{3}} - 1. \tag{8}$$

In particular, we conclude that $t_n = \Theta((1+\sqrt{3})^n)$. Since $s_n = \Theta(4^n)$, this implies that $t_n = o(s_n)$. So the second procedure for moving a stack of n disks is significantly more efficient than the first one.

The derivation of (8) is similar to the one for s_n:

$$\begin{array}{rcccccccc}
T(x) & = & t_0 & + & t_1 x & + & t_2 x^2 & + & t_3 x^3 + \cdots. \\
-2xT(x) & = & & - & 2t_0 x & - & 2t_1 x^2 & - & 2t_2 x^3 - \cdots. \\
-2x^2 T(x) & = & & & & - & 2t_0 x^2 & - & 2t_1 x^3 - \cdots. \\
-3/(1-x) & = & -3 & - & 3x & - & 3x^2 & - & 3x^3 - \cdots. \\
\hline
T(x)(1-2x-2x^2) - \frac{3}{1-x} & = & t_0 - 3 & + & (t_1 - 2t_0 - 3)\,x & + & 0x^2 & + & 0x^3 + \cdots \\
& = & -3 & + & (-2)x. & & & &
\end{array}$$

so

$$\begin{aligned}
T(x)(1-2x-2x^2) &= \frac{3}{1-x} - 3 - 2x \\
&= \frac{2x^2 + x}{1-x},
\end{aligned}$$

and

$$T(x) = \frac{2x^2+x}{(1-x)(1-2x-2x^2)} = \frac{2x^2+x}{(1-x)(1-\alpha x)(1-\beta x)} \tag{9}$$

where $\alpha = 1+\sqrt{3}$, $\beta = 1-\sqrt{3}$. This implies that $T(x)$ can be expressed using partial fractions as

$$T(x) = \frac{a}{1-\alpha x} + \frac{b}{1-\beta x} + \frac{c}{1-x} \tag{10}$$

To find a, b, c, multiply both sides of (10) by $(1-\alpha x)(1-\beta x)(1-x)$ to get

$$2x^2 + x = a(1-\beta x)(1-x) + b(1-\alpha x)(1-x) + c(1-\alpha x)(1-\beta x). \tag{11}$$

Letting $x = 1$ gives

$$3 = c(1-\alpha)(1-\beta) = c(-3)$$

so $c = -1$. Similarly, letting $x = 1/\alpha$ gives (after a little calculation) $a = 1/(3-\sqrt{3})$, and letting $x = 1/\beta$ gives $b = 1/(3+\sqrt{3})$.

Finally, since

$$[x^n]\,(d/(1-\delta x)) = d\delta^n,$$

we conclude that

$$\begin{aligned}
t_n &= a\alpha^n + b\beta n + c1^n \\
&= \frac{1}{3-\sqrt{3}}(1+\sqrt{3})^n + \frac{1}{3+\sqrt{3}}(1-\sqrt{3})^n - 1
\end{aligned}$$

■

Appendix

Let $[x^n]F(x)$ denote the coefficient of x^n in the power series for $F(x)$. Then,

$$[x^n]\left(\frac{1}{(1-\alpha x)^k}\right) = \binom{n+k-1}{k-1}\alpha^n. \tag{12}$$

Partial Fractions

Here's a particular case of the Partial Fraction Rule that should be enough to illustrate the general Rule. Let

$$r(x) ::= \frac{p(x)}{(1-\alpha x)^2(1-\beta x)(1-\gamma x)^3}$$

where α, β, γ are distinct complex numbers, and $p(x)$ is a polynomial of degree less than the demoninator, namely, less than 6. Then there are unique numbers $a_1, a_2, b, c_1, c_2, c_3 \in \mathbb{C}$ such that

$$r(x) = \frac{a_1}{1-\alpha x} + \frac{a_2}{(1-\alpha x)^2} + \frac{b}{1-\beta x} + \frac{c_1}{1-\gamma x} + \frac{c_2}{(1-\gamma x)^2} + \frac{c_3}{(1-\gamma x)^3}$$

Finding a Generating Function for Fibonacci Numbers

The Fibonacci numbers are defined by:

$$\begin{aligned} f_0 &::= 0 \\ f_1 &::= 1 \\ f_n &::= f_{n-1} + f_{n-2} \qquad (\text{for } n \geq 2) \end{aligned}$$

Let F be the generating function for the Fibonacci numbers, that is,

$$F(x) ::= f_0 + f_1 x + f_2 x^2 + f_3 x^3 + \cdots$$

Now we have

$$\begin{array}{rcccccccccc} F(x) & = & f_0 & + & f_1 x & + & f_2 x^2 & + & f_3 x^3 & + \cdots . \\ -xF(x) & = & & - & f_0 x & - & f_1 x^2 & - & f_2 x^3 & - \cdots . \\ -x^2F(x) & = & & & & - & f_0 x^2 & - & f_1 x^3 & - \cdots . \\ \hline F(x)(1-x-x^2) & = & f_0 & + & (f_1 - f_0)x & + & 0x^2 & + & 0x^3 & + \cdots . \\ & = & 0 & + & 1x. & & & & & \end{array}$$

so

$$F(x) = \frac{x}{1-x-x^2}\,.$$

6.042J / 18.062J Mathematics for Computer Science
Spring 2010

Solutions to In-Class Problems Week 12, Wed.

Problem 1.
[A Baseball Series]
The New York Yankees and the Boston Red Sox are playing a two-out-of-three series. (In other words, they play until one team has won two games. Then that team is declared the overall winner and the series ends.) Assume that the Red Sox win each game with probability $3/5$, regardless of the outcomes of previous games.

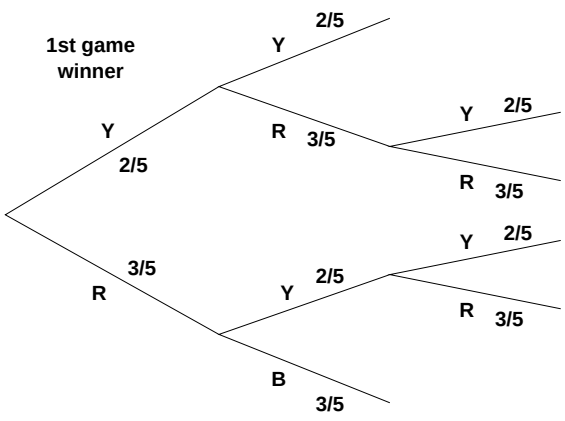
Answer the questions below using the four step method. You can use the same tree diagram for all three problems.

(a) What is the probability that a total of 3 games are played?

(b) What is the probability that the winner of the series loses the first game?

(c) What is the probability that the *correct* team wins the series?

Solution. A tree diagram is worked out below.



outcome	3 games played?	winner lost first game?	correct team wins?	Probability
YY				4/25
YRY	X			12/125
YRR	X	X	X	18/125
RYY	X	X		12/125
RYR	X		X	18/125
RR			X	9/25

From the tree diagram, we get:

$$\Pr\{\text{3 games played}\} = \frac{12}{125} + \frac{18}{125} + \frac{12}{125} + \frac{18}{125} = \frac{12}{25}$$

$$\Pr\{\text{winner lost first game}\} = \frac{18}{125} + \frac{12}{125} = \frac{6}{25}$$

$$\Pr\{\text{correct team wins}\} = \frac{18}{125} + \frac{18}{125} + \frac{9}{25} = \frac{81}{125}$$

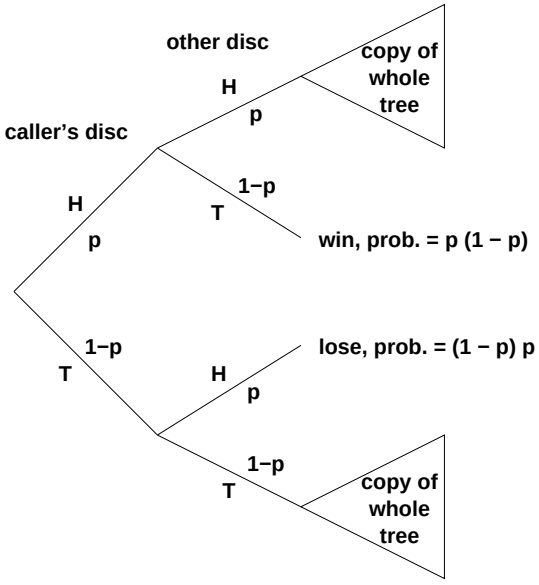
■

Problem 2.
To determine which of two people gets a prize, a coin is flipped twice. If the flips are a Head and then a Tail, the first player wins. If the flips are a Tail and then a Head, the second player wins. However, if both coins land the same way, the flips don't count and whole the process starts over.

Assume that on each flip, a Head comes up with probability p, regardless of what happened on other flips. Use the four step method to find a simple formula for the probability that the first player wins. What is the probability that neither player wins?

Suggestions: The tree diagram and sample space are infinite, so you're not going to finish drawing the tree. Try drawing only enough to see a pattern. Summing all the winning outcome probabilities directly is difficult. However, a neat trick solves this problem and many others. Let s be the sum of all winning outcome probabilities in the whole tree. Notice that *you can write the sum of all the winning probabilities in certain subtrees as a function of* s. Use this observation to write an equation in s and then solve.

Solution. In the tree diagram below, the small triangles represent subtrees that are themselves complete copies of the whole tree.



Let s equal the sum of all winning probabilities in the whole tree. There are two extra edges with probability p on the path to each outcome in the top subtree. Therefore, the sum of winning probabilities in the upper tree is $p^2 s$. Similarly, the sum of winning probabilities in the lower subtree is $(1-p)^2 s$. This gives the equation:

$$s = p^2 s + (1-p)^2 s + p(1-p)$$

The solution to this equation is $s = 1/2$, for all p between 0 and 1.

By symmetry, the probability that the first player loses is $1/2$. This means that the event, if any, of flipping forever can only have probability zero.

Formally, the sample space is the (infinite) set of leaves of the tree, namely,

$$\mathcal{S} ::= \{\mathtt{TT}, \mathtt{HH}\}^* \cdot \{\mathtt{HT}, \mathtt{TH}\}$$

where $\{\mathtt{TT}, \mathtt{HH}\}^*$ denotes the set of strings formed by concatenating a sequence of HH's and TT's. For example,

$$\mathtt{TTTTHHHT}, \mathtt{HHTTTH}, \mathtt{HHHHHHHHHT}, \mathtt{HT} \in \mathcal{S}.$$

For any string $s \in \mathcal{S}$,

$$\Pr\{s\} ::= p^{\#\mathtt{H}\text{'s in } s}(1-p)^{\#\mathtt{T}\text{'s in } s}.$$

To verify that is defines a probability space, we must show that $\sum_{s\in\mathcal{S}} \Pr\{s\} = 1$:

$$\begin{aligned}
\sum_{s\in\mathcal{S}} \Pr\{s\} &= \sum_{n\geq 0} \sum_{s\in\mathcal{S}, |s|=2n+2} p^{\#\mathtt{H}\text{'s in } s}(1-p)^{\#\mathtt{T}\text{'s in } s} \\
&= \sum_{n\geq 0} \sum_{i+j=n} p^{2i}(1-p)^{2j}p(1-p) && \text{(strings that end in HT)} \\
&\quad + \sum_{n\geq 0} \sum_{i+j=n} p^{2i}(1-p)^{2j}p(1-p) && \text{(strings that end in TH)} \\
&= 2p(1-p)\sum_{n\in\mathbb{N}} \left(p^2 + (1-p)^2\right)^n \\
&= \frac{2p(1-p)}{1-(p^2+(1-p)^2)} \\
&= \frac{2p(1-p)}{2p^2+2p} = 1.
\end{aligned}$$

■

Problem 3.
Suppose there is a system with n components, and we know from past experience that any particular component will fail in a given year with probability p. That is, letting F_i be the event that the ith component fails within one year, we have

$$\Pr\{F_i\} = p$$

for $1 \leq i \leq n$. The *system* will fail if *any one* of its components fails. What can we say about the probability that the system will fail within one year?

Let F be the event that the system fails within one year. Without any additional assumptions, we can't get an exact answer for $\Pr\{F\}$. However, we can give useful upper and lower bounds, namely,

$$p \leq \Pr\{F\} \leq np. \tag{1}$$

We may as well assume $p < 1/n$, since the upper bound is trivial otherwise. For example, if $n = 100$ and $p = 10^{-5}$, we conclude that there is at most one chance in 1000 of system failure within a year and at least one chance in 100,000.

Let's model this situation with the sample space $\mathcal{S} ::= \mathcal{P}(\{1, \ldots, n\})$ whose outcomes are subsets of positive integers $\leq n$, where $s \in \mathcal{S}$ corresponds to the indices of exactly those components that fail within one year. For example, $\{2, 5\}$ is the outcome that the second and fifth components failed within a year and none of the other components failed. So the outcome that the system did not fail corresponds to the emptyset, $\emptyset$.

(a) Show that the probability that the system fails could be as small as p by describing appropriate probabilities for the outcomes. Make sure to verify that the sum of your outcome probabilities is 1.

Solution. There could be a probability p of system failure if all the individual failures occur together. That is, let $\Pr\{\{1, \ldots, n\}\} ::= p$, $\Pr\{\emptyset\} ::= 1 - p$, and let the probability of all other outcomes be zero. So $F_i = \{s \in \mathcal{S} \mid i \in s\}$ and $\Pr\{F_i\} = 0 + 0 + \cdots + 0 + \Pr\{\{1, \ldots, n\}\} = \Pr\{\{1, \ldots, n\}\} = p$. Also, the only outcome with positive probability in F is $\{1, \ldots, n\}$, so $\Pr\{F\} = p$, as required. ■

(b) Show that the probability that the system fails could actually be as large as np by describing appropriate probabilities for the outcomes. Make sure to verify that the sum of your outcome probabilities is 1.

Solution. Suppose at most one component ever fails at a time. That is, $\Pr\{\{i\}\} = p$ for $1 \leq i \leq n$, $\Pr\{\emptyset\} = 1 - np$, and probability of all other outcomes is zero. The sum of the probabilities of all the outcomes is one, so this is a well-defined probability space. Also, the only outcome in F_i with positive probability is $\{i\}$, so $\Pr\{F_i\} = \Pr\{\{i\}\} = p$ as required. Finally, $\Pr\{F\} = np$ because $F = \{A \subseteq \{1, \ldots, n\} \mid A \neq \emptyset\}$, so F in particular contains all the n outcomes of the form $\{i\}$. ■

(c) Prove inequality (1). You may assume the Union Bound in the Appendix.

Solution. $F = \bigcup_{i=1}^{n} F_i$ so

$$
\begin{aligned}
p &= \Pr\{F_1\} && \text{(given)} && (2)\\
&\leq \Pr\{F\} && \text{(since } F_1 \subseteq F\text{)} && (3)\\
&= \Pr\left\{\bigcup F_i\right\} && \text{(def. of } F\text{)} && (4)\\
&\leq \sum_{i=1}^{n} \Pr\{F_i\} && \text{(Union Bound)} && (5)\\
&= np. && \text{(since the } F_i\text{'s are disjoint)} && (6)
\end{aligned}
$$

■

Problem 4.
Here are some handy rules for reasoning about probabilities that all follow directly from the Disjoint Sum Rule in the Appendix. Prove them.

$$\Pr\{A - B\} = \Pr\{A\} - \Pr\{A \cap B\} \qquad \text{(Difference Rule)}$$

Solution. Any set A is the disjoint union of $A - B$ and $A \cap B$, so

$$\Pr\{A\} = \Pr\{A - B\} + \Pr\{A \cap B\}$$

by the Disjoint Sum Rule. ■

$$\Pr\left\{\overline{A}\right\} = 1 - \Pr\{A\} \qquad \text{(Complement Rule)}$$

Solution. $\overline{A} ::= \mathcal{S} - A$, so by the Difference Rule

$$\Pr\left\{\overline{A}\right\} = \Pr\{\mathcal{S}\} - \Pr\{A\} = 1 - \Pr\{A\}.$$

■

$$\Pr\{A \cup B\} = \Pr\{A\} + \Pr\{B\} - \Pr\{A \cap B\} \qquad \text{(Inclusion-Exclusion)}$$

Solution. $A \cup B$ is the disjoint union of A and $B - A$ so

$$\begin{aligned} \Pr\{A \cup B\} &= \Pr\{A\} + \Pr\{B - A\} && \text{(Disjoint Sum Rule)} \\ &= \Pr\{A\} + (\Pr\{B\} - \Pr\{A \cap B\}) && \text{(Difference Rule)} \end{aligned}$$

■

$$\Pr\{A \cup B\} \leq \Pr\{A\} + \Pr\{B\}. \qquad \text{(2-event Union Bound)}$$

Solution. This follows immediately from Inclusion-Exclusion and the fact that $\Pr\{A \cap B\} \geq 0$. ■

$$\text{If } A \subseteq B, \text{ then } \Pr\{A\} \leq \Pr\{B\}. \qquad \text{(Monotonicity)}$$

Solution.

$$\begin{aligned} \Pr\{A\} &= \Pr\{B\} - (\Pr\{B\} - \Pr\{A\}) \\ &= \Pr\{B\} - (\Pr\{B\} - \Pr\{A \cap B\}) && (\text{since } A = A \cap B) \\ &= \Pr\{B\} - \Pr\{B - A\} && (\text{difference rule}) \\ &\leq \Pr\{B\} && (\text{since } \Pr\{B - A\} \geq 0). \end{aligned}$$

■

6.042J / 18.062J Mathematics for Computer Science
Spring 2010

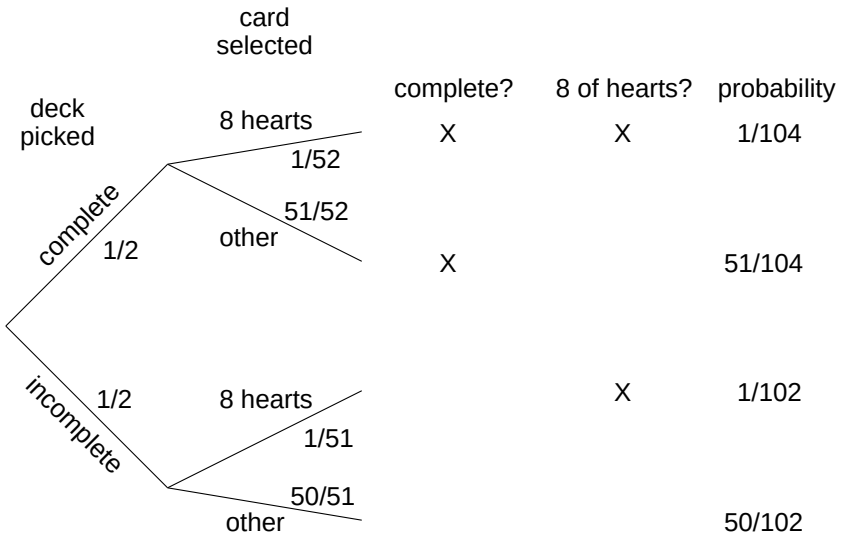
Solutions to In-Class Problems Week 12, Fri.

Problem 1.
There are two decks of cards. One is complete, but the other is missing the ace of spades. Suppose you pick one of the two decks with equal probability and then select a card from that deck uniformly at random. What is the probability that you picked the complete deck, given that you selected the eight of hearts? Use the four-step method and a tree diagram.

Solution. Let C be the event that you pick the complete deck, and let H be the event that you select the eight of hearts. In these terms, our aim is to compute:

$$\Pr\{C \mid H\} = \frac{\Pr\{C \cap H\}}{\Pr\{H\}}$$

A tree diagram is worked out below:



Now we can compute the desired conditional probability as follows:

$$\begin{aligned}\Pr\{C \mid H\} &= \frac{\Pr\{C \cap H\}}{\Pr\{H\}} \\ &= \frac{\frac{1}{2}\cdot\frac{1}{52}}{\frac{1}{2}\cdot\frac{1}{52}+\frac{1}{2}\cdot\frac{1}{51}} \\ &= \frac{51}{103} \\ &= 0.495146\ldots\end{aligned}$$

Thus, if you selected the eight of hearts, then the deck you picked is less likely to be the complete one. It's worth thinking about how you might have arrived at this final conclusion without going through the detailed calculation.

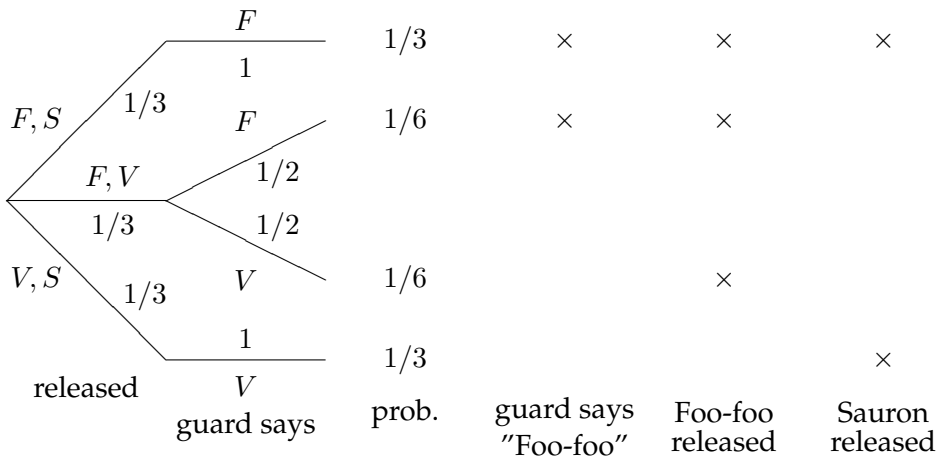
■

Problem 2.
There are three prisoners in a maximum-security prison for fictional villains: the Evil Wizard Voldemort, the Dark Lord Sauron, and Little Bunny Foo-Foo. The parole board has declared that it will release two of the three, chosen uniformly at random, but has not yet released their names. Naturally, Sauron figures that he will be released to his home in Mordor, where the shadows lie, with probability $2/3$.

A guard offers to tell Sauron the name of one of the other prisoners who will be released (either Voldemort or Foo-Foo). Sauron knows the guard to be a truthful fellow. However, Sauron declines this offer. He reasons that if the guard says, for example, "Little Bunny Foo-Foo will be released", then his own probability of release will drop to $1/2$. This is because he will then know that either he or Voldemort will also be released, and these two events are equally likely.

Using a tree diagram and the four-step method, either prove that the Dark Lord Sauron has reasoned correctly or prove that he is wrong. Assume that if the guard has a choice of naming either Voldemort or Foo-Foo (because both are to be released), then he names one of the two uniformly at random.

Solution. Sauron has reasoned incorrectly. In order to understand his error, let's begin by working out the sample space, noting events of interest, and computing outcome probabilities:



Define the events S, F, and "F" as follows:

$$\begin{aligned} \text{"}F\text{"} &= \text{Guard says Foo-Foo is released} \\ F &= \text{Foo-Foo is released} \\ S &= \text{Sauron is released} \end{aligned}$$

The outcomes in each of these events are noted in the tree diagram.

Sauron's error is in failing to realize that the event F (Foo-foo will be released) is different from the event "F" (the guard *says* Foo-foo will be released). In particular, the probability that Sauron is released, given that Foo-foo is released, is indeed $1/2$:

$$\begin{aligned} \Pr\{S \mid F\} &= \frac{\Pr\{S \cap F\}}{\Pr\{F\}} \\ &= \frac{\frac{1}{3}}{\frac{1}{3}+\frac{1}{6}+\frac{1}{6}} \\ &= \frac{1}{2} \end{aligned}$$

But the probability that Sauron is released given that the guard merely *says so* is still $2/3$:

$$\begin{aligned} \Pr\{S \mid \text{"}F\text{"}\} &= \frac{\Pr\{S \cap \text{"}F\text{"}\}}{\Pr\{\text{"}F\text{"}\}} \\ &= \frac{\frac{1}{3}}{\frac{1}{3}+\frac{1}{6}} \\ &= \frac{2}{3} \end{aligned}$$

So Sauron's probability of release is actually unchanged by the guard's statement. ■

Problem 3.
Suppose that you flip three fair, mutually independent coins. Define the following events:

- Let A be the event that *the first* coin is heads.

- Let B be the event that *the second* coin is heads.
- Let C be the event that *the third* coin is heads.
- Let D be the event that *an even number of* coins are heads.

(a) Use the four step method to determine the probability space for this experiment and the probability of each of A, B, C, D.

Solution. The tree is a binary tree with depth 3 and 8 leaves. The successive levels branching to show whether or not the successive events A, B, C occur. By definition of *fair* and *independent*, each branch out of a vertex is equally likely to be followed. So the probability space has as outcomes the eight length-3 strings of `H`'s and `T`'s, each of which has probability $(1/2)^3 = 1/8$.

Each of the events events A, B, C, D are true in four of the outcomes and hence has probability $1/2$. ■

(b) Show that these events are not mutually independent.

Solution.

$$\Pr\{A \cap B \cap C \cap D\} = 0 \neq (1/2)^4 = \Pr\{A\} \cdot \Pr\{B\} \cdot \Pr\{C\} \cdot \Pr\{D\}.$$

■

(c) Show that they are 3-way independent.

Solution. Because the coin tosses are mutually independent, we know:

$$\Pr\{A \cap B \cap C\} = \Pr\{A\} \cdot \Pr\{B\} \cdot \Pr\{C\}.$$

What remains is to check that equality holds for the other subsets of three events: $\{A, B, D\}$, $\{A, C, D\}$, and $\{B, C, D\}$. By symmetry, again, we need only check one, say the first one.

$$\Pr\{A \cap B \cap D\} = \Pr\{\{HHT\}\} = \frac{1}{8}.$$

Since this is equal to $\Pr\{A\} \cdot \Pr\{B\} \cdot \Pr\{D\}$, these three events are independent.

We conclude that all four events are three-way independent. ■

6.042J / 18.062J Mathematics for Computer Science
Spring 2010

Solutions to In-Class Problems Week 13, Mon.

Problem 1.
Suppose there is a system with n components, and we know from past experience that any particular component will fail in a given year with probability p. That is, letting F_i be the event that the ith component fails within one year, we have

$$\Pr\{F_i\} = p$$

for $1 \leq i \leq n$. The *system* will fail if *any one* of its components fails. What can we say about the probability that the system will fail within one year?

Let F be the event that the system fails within one year. Without any additional assumptions, we can't get an exact answer for $\Pr\{F\}$. However, we can give useful upper and lower bounds, namely,

$$p \leq \Pr\{F\} \leq np. \tag{1}$$

We may as well assume $p < 1/n$, since the upper bound is trivial otherwise. For example, if $n = 100$ and $p = 10^{-5}$, we conclude that there is at most one chance in 1000 of system failure within a year and at least one chance in 100,000.

Let's model this situation with the sample space $\mathcal{S} ::= \mathcal{P}(\{1, \ldots, n\})$ whose outcomes are subsets of positive integers $\leq n$, where $s \in \mathcal{S}$ corresponds to the indices of exactly those components that fail within one year. For example, $\{2, 5\}$ is the outcome that the second and fifth components failed within a year and none of the other components failed. So the outcome that the system did not fail corresponds to the emptyset, $\emptyset$.

(a) Show that the probability that the system fails could be as small as p by describing appropriate probabilities for the outcomes. Make sure to verify that the sum of your outcome probabilities is 1.

Solution. There could be a probability p of system failure if all the individual failures occur together. That is, let $\Pr\{\{1, \ldots, n\}\} ::= p$, $\Pr\{\emptyset\} ::= 1 - p$, and let the probability of all other outcomes be zero. So $F_i = \{s \in \mathcal{S} \mid i \in s\}$ and $\Pr\{F_i\} = 0 + 0 + \cdots + 0 + \Pr\{\{1, \ldots, n\}\} = \Pr\{\{1, \ldots, n\}\} = p$. Also, the only outcome with positive probability in F is $\{1, \ldots, n\}$, so $\Pr\{F\} = p$, as required. ■

(b) Show that the probability that the system fails could actually be as large as np by describing appropriate probabilities for the outcomes. Make sure to verify that the sum of your outcome probabilities is 1.

Solution. Suppose at most one component ever fails at a time. That is, $\Pr\{\{i\}\} = p$ for $1 \leq i \leq n$, $\Pr\{\emptyset\} = 1 - np$, and probability of all other outcomes is zero. The sum of the probabilities of all the outcomes is one, so this is a well-defined probability space. Also, the only outcome in F_i with positive probability is $\{i\}$, so $\Pr\{F_i\} = \Pr\{\{i\}\} = p$ as required. Finally, $\Pr\{F\} = np$ because $F = \{A \subseteq \{1, \ldots, n\} \mid A \neq \emptyset\}$, so F in particular contains all the n outcomes of the form $\{i\}$. ■

(c) Prove inequality (1).

Solution. $F = \bigcup_{i=1}^{n} F_i$ so

$$
\begin{aligned}
p &= \Pr\{F_1\} && \text{(given)} && (2)\\
&\leq \Pr\{F\} && \text{(since } F_1 \subseteq F\text{)} && (3)\\
&= \Pr\left\{\bigcup F_i\right\} && \text{(def. of } F\text{)} && (4)\\
&\leq \sum_{i=1}^{n} \Pr\{F_i\} && \text{(Union Bound)} && (5)\\
&= np. && \text{(since the } F_i\text{'s are disjoint)} && (6)
\end{aligned}
$$

■

(d) Describe probabilities for the outcomes so that the component failures are mutually independent.

Solution.

$$\Pr\{s\} ::= p^{|s|}(1-p)^{n-|s|}$$

■

Guess the Bigger Number Game

Team 1:

- Write different integers between 0 and 7 on two pieces of paper.
- Put the papers face down on a table.

Team 2:

- Turn over one paper and look at the number on it.
- Either stick with this number or switch to the unseen other number.

Team 2 wins if it chooses the larger number.

Problem 2.
In section 20.2.3, Team 2 was shown to have a strategy that wins $4/7$ of the time no matter how Team 1 plays. Can Team 2 do better? The answer is "no," because Team 1 has a strategy that guarantees that it wins at least $3/7$ of the time, no matter how Team 2 plays. Describe such a strategy for Team 1 and explain why it works.

Solution. Team 1 should randomly choose a number $Z \in \{0, \ldots, 6\}$ and write Z and $Z+1$ on the pieces of paper with all numbers equally likely.

To see why this works, let N be the number on the paper that Team 2 turns over, and let OK be the event that $N \in \{1, \ldots, 6\}$. So given event OK, that is, given that $N \in \{1, \ldots, 6\}$, Team 1's strategy ensures that half the time N is the higher number and half the time N is the lower number. So given event OK, the probability that Team 1 wins is exactly $1/2$ *no matter how Team 2 chooses to play* (stick or switch).

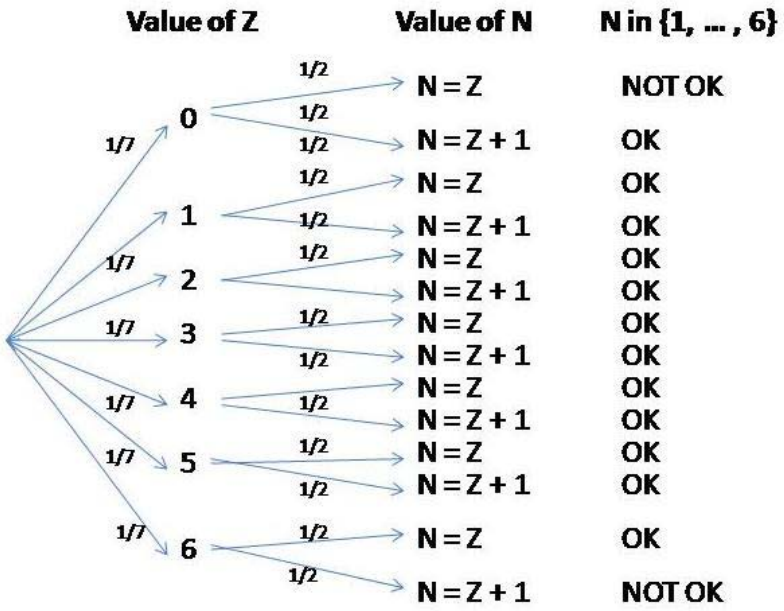
Now we claim that

$$\Pr\{\text{OK}\} = \frac{6}{7}, \tag{7}$$

which implies that the probability that Team 1 wins is indeed at least $(1/2)(6/7) = 3/7$.

To prove $\Pr\{\text{OK}\} = 6/7$, we can follow the four step method. (Note that we couldn't apply this method to model the behavior of Team 2, since we don't know how they may play, and so we can't let our analysis depend on what they do.)

The first level of the probability tree for this game will describe the value of Z: there are seven branches from the root with equal probability going to first level nodes corresponding to the seven possible values of Z. The second level of the tree describes the choice of the number, N: each of the seven first-level nodes has two branches with equal probability, one branch for the case that $N = Z$ and the other for the case that $N = Z + 1$. So there are 14 outcome (leaf) nodes at the second level of the tree, each with probability $1/14$.



Now only two outcomes are not OK, namely, when $Z = 6$ and $N = 7$, and when $Z = 0$ and $N = 0$. Each of the other twelve outcomes is OK, and since each has probability $1/14$, we conclude that $\Pr\{\text{OK}\} = 12/14 = 6/7$, as claimed. ■

Problem 3.
Suppose X_1, X_2, and X_3 are three mutually independent random variables, each having the uniform distribution

$$\Pr\{X_i = k\} \text{ equal to } 1/3 \text{ for each of } k = 1, 2, 3.$$

Let M be another random variable giving the maximum of these three random variables. What is the density function of M?

Solution.

$$\begin{aligned} \text{PDF}_M(1) &= \tfrac{1}{27} \\ \text{PDF}_M(2) &= \tfrac{7}{27} \\ \text{PDF}_M(3) &= \tfrac{19}{27} \end{aligned}$$

This can be hashed out by counting the possible outcomes. Alternatively, we can reason as follows:

The event $M = 1$ is the event that all three of the variables equal 1, and since they are mutually independent, we have

$$\Pr\{M = 1\} = \Pr\{X_1 = 1\} \cdot \Pr\{X_2 = 1\} \cdot \Pr\{X_3 = 1\} = \left(\frac{1}{3}\right)^3 = \frac{1}{27}.$$

To compute $\Pr\{M = 2\}$, we first compute $\Pr\{M \leq 2\}$. Now the event $[M \leq 2]$ is the event that all three of the variables is at most 2, so by mutual independence we have

$$\Pr\{M \leq 2\} = \Pr\{X_1 \leq 2\} \cdot \Pr\{X_2 \leq 2\} \cdot \Pr\{X_3 \leq 2\} = \left(\frac{2}{3}\right)^3 = \frac{8}{27}.$$

Therefore,

$$\Pr\{M = 2\} = \Pr\{M \leq 2\} - \Pr\{M = 1\} = \frac{8}{27} - \frac{1}{27} = \frac{7}{27}.$$

Finally,

$$\Pr\{M = 3\} = 1 - \Pr\{M \leq 2\} = 1 - \frac{8}{27} = \frac{19}{27}.$$

■

Problem 4.
Suppose you have a biased coin that has probability p of flipping heads. Let J be the number of heads in n independent coin flips. So J has the general binomial distribution:

$$\text{PDF}_J(k) = \binom{n}{k} p^k q^{n-k}$$

where $q ::= 1 - p$.

(a) Show that

$$\begin{aligned} \text{PDF}_J(k) &< \text{PDF}_J(k+1) && \text{for } k < np + p, \\ \text{PDF}_J(k) &> \text{PDF}_J(k+1) && \text{for } k > np + p. \end{aligned}$$

Solution. Consider the ratio of the probability of k heads over the probability of $k-1$ heads.

$$\begin{aligned} \frac{\text{PDF}_J(k)}{\text{PDF}_J(k-1)} &= \frac{\binom{n}{k} p^k q^{n-k}}{\binom{n}{k-1} p^{k-1} q^{n-k+1}} \\ &= \frac{\frac{n!}{k!\,(n-k)!}}{\frac{n!}{(k-1)!\,(n-k+1)!}} \frac{p}{q} \\ &= \frac{(n-k+1)p}{kq} \end{aligned}$$

This fraction is greater than 1 precisely when $(n-k+1)p > kq = k(1-p)$, that is when $k < np+p$. So for $k < np + p$, the probability of k heads increases as k increases, and for $k > np + p$, the probability decreases as k increases. ■

(b) Conclude that the maximum value of PDF_J is asymptotically equal to

$$\frac{1}{\sqrt{2\pi npq}}.$$

Hint: For the asymptotic estimate, it's ok to assume that np is an integer, so by part (a) the maximum value is $\text{PDF}_J(np)$. Use Stirling's formula 15.12[1].

[1] $n! \sim \left(\frac{n}{e}\right)^n \sqrt{2\pi n}$

Solution.

$$\begin{aligned}
\mathrm{PDF}_J(np) ::&= \binom{n}{np} p^{np} q^{n-np} \\
&= \frac{n!}{(np)!\,(nq)!} p^{np} q^{nq} \\
&\sim \frac{\left(\frac{n}{e}\right)^n \sqrt{2\pi n}}{\left(\left(\frac{np}{e}\right)^{np} \sqrt{2\pi np}\right)\left(\left(\frac{nq}{e}\right)^{nq} \sqrt{2\pi nq}\right)} p^{np} q^{nq} \\
&= \frac{\frac{n^n}{e^n}\sqrt{2\pi n}}{\left(\frac{n^{np}p^{np}}{e^{np}}\sqrt{2\pi np}\right)\left(\frac{n^{nq}q^{nq}}{e^{nq}}\sqrt{2\pi nq}\right)} p^{np} q^{nq} \\
&= \frac{\frac{n^n}{e^n}\sqrt{2\pi n}}{\frac{n^{np+nq}p^{np}q^{nq}}{e^{np+nq}}\sqrt{2\pi np}\sqrt{2\pi nq}} p^{np} q^{nq} p^{np} q^{nq} \\
&= \frac{\frac{n^n}{e^n}\sqrt{2\pi n}}{\frac{n^n}{e^n}\sqrt{2\pi np}\sqrt{2\pi nq}} \\
&= \frac{1}{\sqrt{2\pi npq}}.
\end{aligned}$$

■

6.042J / 18.062J Mathematics for Computer Science
Spring 2010

Solutions to In-Class Problems Week 13, Wed.

Problem 1.
Let's see what it takes to make Carnival Dice fair. Here's the game with payoff parameter k: make three independent rolls of a fair die. If you roll a six

- no times, then you lose 1 dollar.
- exactly once, then you win 1 dollar.
- exactly twice, then you win two dollars.
- all three times, then you win k dollars.

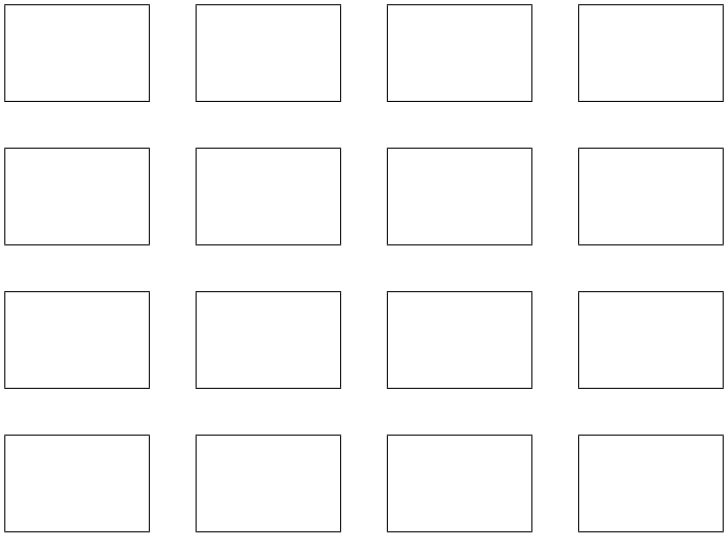
For what value of k is this game fair?

Solution. Let the random variable P be your payoff. Then we can compute $\mathrm{E}[P]$ as follows:

$$\begin{aligned}\mathrm{E}[P] &= -1 \cdot \Pr\{0 \text{ sixes}\} + 1 \cdot \Pr\{1 \text{ six}\} + 2 \cdot \Pr\{2 \text{ sixes}\} + k \cdot \Pr\{3 \text{ sixes}\} \\ &= -1 \cdot \left(\frac{5}{6}\right)^3 + 1 \cdot 3\left(\frac{1}{6}\right)\left(\frac{5}{6}\right)^2 + 2 \cdot 3\left(\frac{1}{6}\right)^2\left(\frac{5}{6}\right) + k \cdot \left(\frac{1}{6}\right)^3 \\ &= \frac{-125 + 75 + 30 + k}{216}\end{aligned}$$

The game is fair when $\mathrm{E}[P] = 0$. This happens when $k = 20$. ■

Problem 2.
A classroom has sixteen desks arranged as shown below.



If there is a girl in front, behind, to the left, or to the right of a boy, then the two of them *flirt*. One student may be in multiple flirting couples; for example, a student in a corner of the classroom can flirt with up to two others, while a student in the center can flirt with as many as four others. Suppose that desks are occupied by boys and girls with equal probability and mutually independently. What is the expected number of flirting couples? *Hint:* Linearity.

Solution. First, let's count the number of pairs of adjacent desks. There are three in each row and three in each column. Since there are four rows and four columns, there are $3 \cdot 4 + 3 \cdot 4 = 24$ pairs of adjacent desks.

Number these pairs of adjacent desks from 1 to 24. Let F_i be an indicator for the event that occupants of the desks in the i-th pair are flirting. The probability we want is then:

$$\begin{aligned} \mathrm{E}\left[\sum_{i=1}^{24} F_i\right] &= \sum_{i=1}^{24} \mathrm{E}\left[F_i\right] && \text{(linearity of } \mathrm{E}\left[\cdot\right]\text{)} \\ &= \sum_{i=1}^{24} \Pr\left\{F_i = 1\right\} && (F_i \text{ is an indicator}) \end{aligned}$$

The occupants of adjacent desks are flirting iff they are of opposite sexes, which happens with probability $1/2$, that is, $\Pr\{F_i = 1\} = 1/2$. Plugging this into the previous expression gives:

$$\mathrm{E}\left[\sum_{i=1}^{24} F_i\right] = \sum_{i=1}^{24} \Pr\left\{F_i = 1\right\} = 24 \cdot \frac{1}{2} = 12$$

■

Problem 3. (a) Suppose we flip a fair coin until two Tails in a row come up. What is the expected number, N_{TT}, of flips we perform? *Hint:* Let D be the tree diagram for this process. Explain why $D = H \cdot D + T \cdot (H \cdot D + T)$. Use the Law of Total Expectation 20.3.5

Solution. $N_{\mathtt{TT}} = 6$.

From D and Total Expectation:

$$N_{\mathtt{TT}} = \frac{1}{2} \cdot [1 + N_{\mathtt{TT}}] + \frac{1}{2} \cdot \left(1 + \frac{1}{2} \cdot [1 + N_{\mathtt{TT}}] + \frac{1}{2} \cdot 1\right)$$

■

(b) Suppose we flip a fair coin until a Tail immediately followed by a Head come up. What is the expected number, $N_{\mathtt{TH}}$, of flips we perform?

Solution. $N_{\mathtt{TH}} = 4$.

This time the tree diagram $C = H \cdot C + T \cdot B$ where the subtree $B = H + T \cdot B$.

So

$$N_{\mathtt{TH}} = \frac{1}{2} \cdot [1 + N_{\mathtt{TH}}] + \frac{1}{2} \cdot [1 + N_B]$$

where N_B is the expected number of flips in the B subtree. But

$$N_B = \frac{1}{2} \cdot 1 + \frac{1}{2} \cdot [1 + N_B].$$

That is, $N_B = 2$. Hence,

$$N_{\mathtt{TH}} = \frac{1}{2} \cdot [1 + 2] + \frac{1}{2} \cdot [1 + N_{\mathtt{TH}}]$$

which implies $N_{\mathtt{TH}} = 4$. ■

(c) Suppose we now play a game: flip a fair coin until either `TT` or `TH` first occurs. You win if `TT` comes up first, lose if `TH` comes up first. Since `TT` takes 50% longer on average to turn up, your opponent agrees that he has the advantage. So you tell him you're willing to play if you pay him \$5 when he wins, but he merely pays you a 20% premium, that is, \$6, when you win.

If you do this, you're sneakily taking advantage of your opponent's untrained intuition, since you've gotten him to agree to unfair odds. What is your expected profit per game?

Solution. It's easy to see that both `TT` and `TH` are equally likely to show up first. (Every game play consists of a sequence of `H`'s followed by a `T`, after which the game ends with a `T` or an `H`, with equal probability.) So your expected profit is

$$\frac{1}{2} \cdot 6 + \frac{1}{2} \cdot (-5)$$

dollars, that is 50 cents per game. So leap to play. ■

Problem 4.

Justify each line of the following proof that if R_1 and R_2 are *independent*, then

$$\mathrm{E}[R_1 \cdot R_2] = \mathrm{E}[R_1] \cdot \mathrm{E}[R_2].$$

Proof.

$$
\begin{aligned}
&\mathrm{E}\left[R_1 \cdot R_2\right] \\
&= \sum_{r \in \text{range}(R_1 \cdot R_2)} r \cdot \Pr\left\{R_1 \cdot R_2 = r\right\} \\
&= \sum_{r_i \in \text{range}(R_i)} r_1 r_2 \cdot \Pr\left\{R_1 = r_1 \text{ and } R_2 = r_2\right\} \\
&= \sum_{r_1 \in \text{range}(R_1)} \sum_{r_2 \in \text{range}(R_2)} r_1 r_2 \cdot \Pr\left\{R_1 = r_1 \text{ and } R_2 = r_2\right\} \\
&= \sum_{r_1 \in \text{range}(R_1)} \sum_{r_2 \in \text{range}(R_2)} r_1 r_2 \cdot \Pr\left\{R_1 = r_1\right\} \cdot \Pr\left\{R_2 = r_2\right\} \\
&= \sum_{r_1 \in \text{range}(R_1)} \left(r_1 \Pr\left\{R_1 = r_1\right\} \cdot \sum_{r_2 \in \text{range}(R_2)} r_2 \Pr\left\{R_2 = r_2\right\} \right) \\
&= \sum_{r_1 \in \text{range}(R_1)} r_1 \Pr\left\{R_1 = r_1\right\} \cdot \mathrm{E}\left[R_2\right] \\
&= \mathrm{E}\left[R_2\right] \cdot \sum_{r_1 \in \text{range}(R_1)} r_1 \Pr\left\{R_1 = r_1\right\} \\
&= \mathrm{E}\left[R_2\right] \cdot \mathrm{E}\left[R_1\right].
\end{aligned}
$$

■

Solution. *Proof.*

$$
\begin{aligned}
&\mathrm{E}\left[R_1 \cdot R_2\right] \\
&::= \sum_{r \in \text{range}(R_1 \cdot R_2)} r \cdot \Pr\left\{R_1 \cdot R_2 = r\right\} && \text{(by definition)} \\
&= \sum_{r_i \in \text{range}(R_i)} r_1 r_2 \cdot \Pr\left\{R_1 = r_1 \text{ AND } R_2 = r_2\right\} && \text{(event } [R_1 \cdot R_2 = r] \text{ splits into events} \\
& && [R_1 = r_1 \text{ AND } R_2 = r_2] \text{ such that } r_1 r_2 = r) \\
&= \sum_{r_1 \in \text{range}(R_1)} \sum_{r_2 \in \text{range}(R_2)} r_1 r_2 \cdot \Pr\left\{R_1 = r_1 \text{ AND } R_2 = r_2\right\} && \text{(ordering terms in the sum)} \\
&= \sum_{r_1 \in \text{range}(R_1)} \sum_{r_2 \in \text{range}(R_2)} r_1 r_2 \cdot \Pr\left\{R_1 = r_1\right\} \cdot \Pr\left\{R_2 = r_2\right\} && \text{(independence of } R_1, R_2) \\
&= \sum_{r_1 \in \text{range}(R_1)} \left(r_1 \Pr\left\{R_1 = r_1\right\} \cdot \sum_{r_2 \in \text{range}(R_2)} r_2 \Pr\left\{R_2 = r_2\right\} \right) && \text{(factor out } r_1 \Pr\left\{R_1 = r_1\right\}) \\
&= \sum_{r_1 \in \text{range}(R_1)} r_1 \Pr\left\{R_1 = r_1\right\} \cdot \mathrm{E}\left[R_2\right] && \text{(def of } \mathrm{E}\left[R_2\right]) \\
&= \mathrm{E}\left[R_2\right] \cdot \sum_{r_1 \in \text{range}(R_1)} r_1 \Pr\left\{R_1 = r_1\right\} && \text{(factor out } \mathrm{E}\left[R_2\right]) \\
&= \mathrm{E}\left[R_2\right] \cdot \mathrm{E}\left[R_1\right]. && \text{(def of } \mathrm{E}\left[R_1\right])
\end{aligned}
$$

■

6.042J / 18.062J Mathematics for Computer Science
Spring 2010

Solutions to In-Class Problems Week 13, Fri.

Problem 1.
A herd of cows is stricken by an outbreak of *cold cow disease*. The disease lowers the normal body temperature of a cow, and a cow will die if its temperature goes below 90 degrees F. The disease epidemic is so intense that it lowered the average temperature of the herd to 85 degrees. Body temperatures as low as 70 degrees, **but no lower**, were actually found in the herd.

(a) Prove that at most $3/4$ of the cows could have survived.

Hint: Let T be the temperature of a random cow. Make use of Markov's bound.

Solution. Let T be the temperature of a random cow. Then the fraction of cows that survive is the probability that $T \geq 90$, and $\mathrm{E}[T]$ is the average temperature of the herd.

Applying Markov's Bound to T:

$$\Pr\{T \geq 90\} =\leq \frac{\mathrm{E}[T]}{90} = \frac{85}{90} = \frac{17}{18}.$$

But $17/18 > 3/4$, so this bound is not good enough.

Instead, we apply Markov's Bound to $T - 70$:

$$\Pr\{T \geq 90\} = \Pr\{T - 70 \geq 20\} \leq \frac{\mathrm{E}[T-70]}{20} = (85-70)/20 = 3/4.$$

■

(b) Suppose there are 400 cows in the herd. Show that the bound of part (a) is best possible by giving an example set of temperatures for the cows so that the average herd temperature is 85, and with probability $3/4$, a randomly chosen cow will have a high enough temperature to survive.

Solution. Let 100 cows have temperature 70 degrees and 300 have 90 degrees. So the probability that a random cow has a high enough temperature to survive is exactly $3/4$. Also, the mean temperature is

$$(1/4)70 + (3/4)90 = 85.$$

So this distribution of temperatures satisfies the conditions under which the Markov bound implies that the probability of having a high enough temperature to survive cannot be larger than $3/4$. ■

Problem 2.
A gambler plays 120 hands of draw poker, 60 hands of black jack, and 20 hands of stud poker per day. He wins a hand of draw poker with probability 1/6, a hand of black jack with probability 1/2, and a hand of stud poker with probability 1/5.

(a) What is the expected number of hands the gambler wins in a day?

Solution. $120(1/6) + 60(1/2) + 20(1/5) = 54$. ■

(b) What would the Markov bound be on the probability that the gambler will win at least 108 hands on a given day?

Solution. The expected number of games won is 54, so by Markov, $\Pr\{R \geq 108\} \leq 54/108 = 1/2$. ■

(c) Assume the outcomes of the card games are pairwise independent. What is the variance in the number of hands won per day?

Solution. The variance can also be calculated using linearity of variance. For an individual hand the variance is $p(1-p)$ where p is the probability of winning. Therefore the variance is

$$120(1/6)(5/6) + 60(1/2)(1/2) + 20(1/5)(4/5) = 523/15 = 34\,\tfrac{13}{15}.$$

■

(d) What would the Chebyshev bound be on the probability that the gambler will win at least 108 hands on a given day? You may answer with a numerical expression that is not completely evaluated.

Solution.

$$\Pr\{R - 54 \geq 54\} \leq \Pr\{|R - 54| \geq 54\} \leq \frac{Var[R]}{54^2} = \frac{523}{15(54)^2} \approx 0.01196.$$

(A very slightly better bound of 0.01182 comes from using the one-sided Chebyshev bound from Problem **??**.)

■

Problem 3.
The proof of the Pairwise Independent Sampling Theorem 21.5.1 was given for a sequence $R_1, R_2, \ldots$ of pairwise independent random variables with the same mean and variance.

The theorem generalizes straighforwardly to sequences of pairwise independent random variables, possibly with *different* distributions, as long as all their variances are bounded by some constant.

Theorem (Generalized Pairwise Independent Sampling)**.** *Let $X_1, X_2, \ldots$ be a sequence of pairwise independent random variables such that* $\text{Var}[X_i] \leq b$ *for some $b \geq 0$ and all $i \geq 1$. Let*

$$A_n ::= \frac{X_1 + X_2 + \cdots + X_n}{n},$$
$$\mu_n ::= \text{E}[A_n].$$

Then for every $\epsilon > 0$,

$$\Pr\{|A_n - \mu_n| > \epsilon\} \leq \frac{b}{\epsilon^2} \cdot \frac{1}{n}. \tag{1}$$

(a) Prove the Generalized Pairwise Independent Sampling Theorem.

Solution. Essentially identical to the proof of Theorem 21.5.1 in the text, except that G gets replaced by X and $\text{Var}[G_i]$ by b, with the equality where the b is first used becoming $\leq$. ■

(b) Conclude that the following holds:
Corollary (Generalized Weak Law of Large Numbers)**.** *For every $\epsilon > 0$,*

$$\lim_{n\to\infty} \Pr\{|A_n - \mu_n| \leq \epsilon\} = 1.$$

Solution.

$$\begin{aligned}\Pr\{|A_n - \mu_n| \leq \epsilon\} &= 1 - \Pr\{|A_n - \mu_n| > \epsilon\} \\ &\geq 1 - b/(n\epsilon^2) \qquad \text{(by (1))},\end{aligned}$$

and for any fixed ϵ, this last term approaches 1 as n approaches infinity. ■

6.042J / 18.062J Mathematics for Computer Science
Spring 2010

Solutions to In-Class Problems Week 14, Mon.

Problem 1.
A recent Gallup poll found that 35% of the adult population of the United States believes that the theory of evolution is "well-supported by the evidence." Gallup polled 1928 Americans selected uniformly and independently at random. Of these, 675 asserted belief in evolution, leading to Gallup's estimate that the fraction of Americans who believe in evolution is $675/1928 \approx 0.350$. Gallup claims a margin of error of 3 percentage points, that is, he claims to be confident that his estimate is within 0.03 of the actual percentage.

(a) What is the largest variance an indicator variable can have?

Solution.

$$\frac{1}{4}$$

By Lemma 21.4.2, Var $[H] = pq$.

Noting that $d\,p(1-p)/dp = 2p - 1$ is zero when $p = 1/2$, it follows that the maximum value of $p(1-p)$ must be at $p = 1/2$, so the maximum value of Var $[H]$ is $(1/2)(1-(1/2)) = 1/4$. ■

(b) Use the Pairwise Independent Sampling Theorem to determine a confidence level with which Gallup can make his claim.

Solution. By the Pairwise Independent Sampling, the probability that a sample of size $n = 1928$ is further than $x = 0.03$ of the actual fraction is at most

$$\left(\frac{\sigma}{x}\right)^2 \cdot \frac{1}{n} \leq \left(\frac{1}{4(0.03)^2} \cdot \frac{1}{1928}\right) \leq 0.144$$

so we can be confident of Gallup's estimate at the 85.6% level. ■

(c) Gallup actually claims greater than 99% confidence in his estimate. How might he have arrived at this conclusion? (Just explain what quantity he could calculate; you do not need to carry out a calculation.)

Solution. Gallup's sample has a binomial distribution $B_{1928,p}$ for an unknown p he estimates to be about 0.35. So he wants an upper bound on

$$\Pr\left\{\left|\frac{B_{1928,p}}{1928} - p\right| > 0.03\right\}$$

By part (a), the variance of $B_{n,p}$ is largest when $p = 1/2$, which suggests that the probability that a sample average differs from the actual mean will be largest when $p = 1/2$. This is in fact the case. So Gallup will calculate

$$\begin{aligned}\Pr\left\{\left|\frac{B_{1928,1/2}}{1928} - \frac{1}{2}\right| > 0.03\right\} &= \Pr\left\{\left|B_{1928,1/2} - \frac{1928}{2}\right| > 0.03(1928)\right\} \\ &= \Pr\left\{906 \le B_{1928,1/2} \le 1021\right\} \\ &= \frac{\sum_{i=906}^{1021}\binom{1928}{i}}{2^{1928}} \approx 0.9912.\end{aligned}$$

Mathematica will actually calculate this sum exactly. There are also simple ways to use Stirling's formula to get a good estimate of this value. ■

(d) Accepting the accuracy of all of Gallup's polling data and calculations, can you conclude that there is a high probability that the number of adult Americans who believe in evolution is 35 ± 3 percent?

Solution. No. As explained in Notes and lecture, the assertion that fraction p is in the range 0.35 ± 0.03 is an assertion of fact that is either true or false. The number p is a *constant*. We don't know its value, and we don't know if the asserted fact is true or false, but there is nothing probabilistic about the fact's truth or falsehood.

We *can* say that either the assertion is true or else a 1-in-100 event occurred during the poll. Specifically, the unlikely event is that Gallup's random sample was unrepresentative. This may convince you that p is "probably" in the range 0.35 ± 0.03, but this informal "probably" is not a mathematical probability. ■

Problem 2.
Yesterday, the programmers at a local company wrote a large program. To estimate the fraction, b, of lines of code in this program that are buggy, the QA team will take a small sample of lines chosen randomly and independently (so it is possible, though unlikely, that the same line of code might be chosen more than once). For each line chosen, they can run tests that determine whether that line of code is buggy, after which they will use the fraction of buggy lines in their sample as their estimate of the fraction b.

The company statistician can use estimates of a binomial distribution to calculate a value, s, for a number of lines of code to sample which ensures that with 97% confidence, the fraction of buggy lines in the sample will be within 0.006 of the actual fraction, b, of buggy lines in the program.

Mathematically, the *program* is an actual outcome that already happened. The *sample* is a random variable defined by the process for randomly choosing s lines from the program. The justification for the statistician's confidence depends on some properties of the program and how the sample of s lines of code from the program are chosen. These properties are described in some of the statements below. Indicate which of these statements are true, and explain your answers.

1. The probability that the ninth line of code in the *program* is buggy is b.

Solution. False.

The program has already been written, so there's nothing probabilistic about the buggyness of the ninth (or any other) line of the program: either it is or it isn't buggy, though we don't know which. You could argue that this means it is buggy with probability zero or one, but in any case, it certainly isn't b. ■

2. The probability that the ninth line of code chosen for the *sample* is defective, is b.

Solution. True.

The ninth line sampled is equally likely to be any line of the program, so the probability it is buggy is the same as the fraction, b, of buggy lines in the program. ■

3. All lines of code in the program are equally likely to be the third line chosen in the *sample*.

Solution. True.

The meaning of "random choices of lines from the program" is precisely that at each of the s choices in the sample, in particular at the third choice, each line in the program is equally likely to be chosen. ■

4. Given that the first line chosen for the *sample* is buggy, the probability that the second line chosen will also be buggy is greater than b.

Solution. False.

The meaning of "*independent* random choices of lines from the program" is precisely that at each of the s choices in the sample, in particular at the second choice, each line in the program is equally likely to be chosen, independent of what the first or any other choice happened to be. ■

5. Given that the last line in the *program* is buggy, the probability that the next-to-last line in the program will also be buggy is greater than b.

Solution. False.

As noted above, it's zero or one. ■

6. The expectation of the indicator variable for the last line in the *sample* being buggy is b.

Solution. True.

The expectation of the indicator variable is the same as the probability that it is 1, namely, it is the probability that the sth line chosen is buggy, which is b, by the reasoning above. ■

7. Given that the first two lines of code selected in the *sample* are the same kind of statement —they might both be assignment statements, or both be conditional statements, or both loop statements,...—the probability that the first line is buggy may be greater than b.

Solution. True.

We don't know how prone to bugginess different kinds of statements may be. It could be for example, that conditionals are more prone to bugginess than other kinds of statements, and that there are more conditional lines than any other kind of line in the program. Then given that two randomly chosen lines in the sample are the same kind, they are more likely to be conditionals, which makes them more prone to bugginess. That is, the conditional probability that they will be buggy would be greater than b. ■

8. There is zero probability that all the lines in the *sample* will be different.

Solution. False.

We know the length, r, of the program is larger than the "small" sample size, s, in which case the probability that all the lines in the sample are different is

$$\frac{r}{r} \cdot \frac{r-1}{r} \cdot \frac{r-2}{r} \cdots \frac{r-(s-1)}{r} = \frac{r!}{(r-s)!\, r^s} > 0.$$

Of course it would be true by the Pigeonhole Principle if $s > r$. ■

Problem 3.
A defendent in traffic court is trying to beat a speeding ticket on the grounds that —since virtually everybody speeds on the turnpike —the police have unconstitutional discretion in giving tickets to anyone they choose. (By the way, we don't recommend this defense :-))

To support his argument, the defendent arranged to get a random sample of trips by 3,125 cars on the turnpike and found that 94% of them broke the speed limit at some point during their trip. He says that as a consequence of sampling theory (in particular, the Pairwise Independent Sampling Theorem), the court can be 95% confident that the actual percentage of all cars that were speeding is $94 \pm 4\%$.

The judge observes that the actual number of car trips on the turnpike was never considered in making this estimate. He is skeptical that, whether there were a thousand, a million, or 100,000,000 car trips on the turnpike, sampling only 3,125 is sufficient to be so confident.

Suppose you were were the defendent. How would you explain to the judge why the number of randomly selected cars that have to be checked for speeding *does not depend on the number of recorded trips*? Remember that judges are not trained to understand formulas, so you have to provide an intuitive, nonquantitative explanation.

Solution. This was intended to be a thought-provoking, conceptual question. In past terms, although most of the class could follow the derivations and crank through the formulas to calculate sample size and confidence levels, many students couldn't articulate, and indeed didn't really believe that the derived sample sizes were actually adequate to produce reliable estimates.

Here's a way to explain why we model sampling cars as independent coin tosses that might work, though we aren't sure about this.

Of the approximately 36,000,000 recorded turnpike trips by cars in 2009, there were some *unknown* number, say 35,000,000, that broke the speed limit at some point during their trip. So in this case, the *fraction* of speeders is 35,000,000/36,000,000 which is a little over 0.97.

To estimate this unknown fraction, we randomly select some trip from the 36,000,000 recorded in such a way that *every trip has an equal chance of being picked*. Picking a trip to check for speeding this way amounts to rolling a pair dice and checking that double sixes were not rolled —this has exactly the same probability as picking a speeding car.

After we have picked a car trip and checked if it ever broke the speed limit, make another pick, again making sure that every recorded trip is equally likely to be picked the second time, and so on, for picking a bunch of trips. Now each pick is like rolling the dice and checking against double sixes.

Now everyone understands that if we keep rolling dice looking for double sixes, then the longer we roll, the closer the fraction of rolls that are double sixes will be to 1/36, since only 1 out of the 36 possible dice ouotcomes is double six. Mathematical theory lets us calculate us how many times to roll the dice to make the fraction of double sixes very likely close to 1/36, but we needn't go into the details of the calculation.

Now suppose we had a different number of recorded trips, but the same fraction were speeding. Then we could simply use the same dice in the same way to estimate the speeding fraction from this different set of trip records.

So the number of rolls needed does not depend on how many trips were recorded, it just depends on the fraction of recorded speeders.

■

Problem 4.
An *International Journal of Epidemiology* has a policy that they will only publish the results of a drug trial when there were enough patients in the drug trial to be sure that the conclusions about the drug's effectiveness hold at the 95% confidence level. The editors of the Journal reason that under this policy, their readership can be confident that at most 5% of the published studies will be mistaken.

Later, the editors are astonished and embarrassed to learn that *every one* of the 20 drug trial results they published during the year was wrong. This happened even though the editors and reviewers had carefully checked the submitted data, and every one of the trials was *properly performed and reported* in the published paper.

The editors thought the probability of this was negligible (namely, $(1/20)^{20} < 10^{-25}$). Explain what's wrong with their reasoning and how it could be that all 20 published studies were wrong.

Solution. The editors have confused the statistical *confidence level* with *probability*. It's a mistake to think that because the conclusion of *particular* drug trial submitted to the journal holds at the 95% confidence level, this means its conclusion is wrong with probability only 1/20.

The conclusion of the particular submitted drug trial is right or wrong –period. An assertion of 95% confidence means that if very many trails were carried out, we expect that close to 95% of the

trials would yield a correct conclusion. So if the results of all the many trials were all submitted for publication, and the editors selected 20 of these at random to publish, then they could reasonably expect that only one of them would be wrong.

But that's not what happens: not all the trials are written up and submitted, so the confidence level of the trial is not specially relevant. For example, there may be more than 400 worthless "alternative" drugs being tried by proponents who are genuinely honest, even if misguided. When they conduct careful trials with a 95% confidence level, we can expect that in 1/20 of the 400 trials, worthless —even damaging —drugs will look helpful. The remaining 19/20 of the 400 trials would not be submitted for publication by honest proponents because the trials did not show positive results at the 95% level. But the 20 that mistakenly showed positive results might well all be submitted with no intention to mislead.

This is why, unless there is an explanation of *why* a therapy works, scientists and doctors usually doubt results claiming to confirm the efficacy of some mysterious therapy at a high confidence level. ■

6.042J / 18.062J Mathematics for Computer Science
Spring 2010

Solutions to In-Class Problems Week 14, Wed.

Problem 1.
A gambler is placing \$1 bets on the "1st dozen" in roulette. This bet wins when a number from one to twelve comes in, and then the gambler gets his \$1 back plus \$3 more. Recall that there are 38 numbers on the roulette wheel.

The gambler's initial stake in $\$n$ and his target is $\$T$. He will keep betting until he runs out of money ("goes broke") or reachs his target. Let w_n be the probability of the gambler winning, that is, reaching target $\$T$ before going broke.

(a) Write a linear recurrence for w_n; you need *not* solve the recurrence.

Solution. The probability of winning a bet is $12/38$. Thus, by the Law of Total Probability **??**,

$$\begin{aligned} w_n &= \Pr\{\text{win starting with } \$n \mid \text{won first bet}\} \cdot \Pr\{\text{won first bet}\} + \Pr\{\text{win starting with } \$n \mid \text{lost first bet}\} \cdot \Pr \\ &= \Pr\{\text{win starting with } \$n+3\} \cdot \Pr\{\text{won first bet}\} + \Pr\{\text{win starting with } \$n-1\} \cdot \Pr\{\text{lost first bet}\}, \end{aligned}$$

so

$$w_n = \frac{12}{38} w_{n+3} + \frac{26}{38} w_{n-1}.$$

Letting $m ::= n+3$ we get

$$w_m = \frac{38}{12} w_{m-3} - \frac{26}{12} w_{m-4}.$$

■

(b) Let e_n be the expected number of bets until the game ends. Write a linear recurrence for e_n; you need *not* solve the recurrence.

Solution. By the Law of Total Expectation, Theorem **??**,

$$\begin{aligned} e_n &= (1 + \mathrm{E}[\text{number of bets starting with } \$n \mid \text{won first bet}]) \cdot \Pr\{\text{won first bet}\} + (1 + \mathrm{E}[\text{number of bets starting} \\ &= (1 + \mathrm{E}[\text{number of bets starting with } \$n+3]) \cdot \Pr\{\text{won first bet}\} + (1 + \mathrm{E}[\text{number of bets starting with } \$n - \end{aligned}$$

so

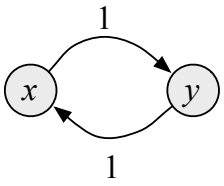
$$e_n = (e_{n+3} + 1)\frac{12}{38} + (1 + e_{n-1})\frac{26}{38}$$

Letting $m ::= n+3$ we get

$$e_m = \frac{38}{12} e_{m-3} - \frac{1 - 26/12}{26/12} \cdot e_{m-4} - \frac{38}{12}$$

■

Problem 2.
Consider the following random-walk graph:



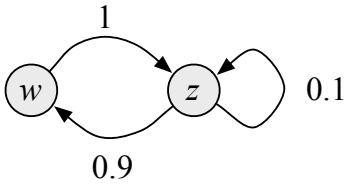
(a) Find a stationary distribution.

Solution. $d(x) = d(y) = 1/2$ ■

(b) If you start at node x and take a (long) random walk, does the distribution over nodes ever get close to the stationary distribution? Explain.

Solution. No! you just alternate between nodes x and y. ■

Consider the following random-walk graph:



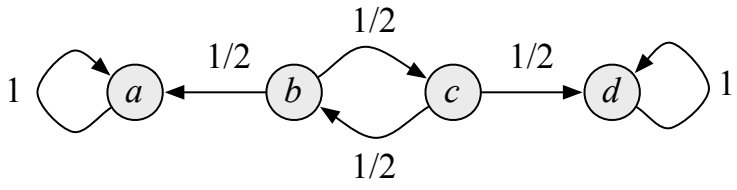
(c) Find a stationary distribution.

Solution. $d(w) = 9/19$, $d(z) = 10/19$. You can derive this by setting $d(w) = (9/10)d(z)$, $d(z) = d(w) + (1/10)d(z)$, and $d(w) + d(z) = 1$. There is a unique solution. ■

(d) If you start at node w and take a (long) random walk, does the distribution over nodes ever get close to the stationary distribution? We don't want you to prove anything here, just write out a few steps and see what's happening.

Solution. Yes, it does. ■

Consider the following random-walk graph:



(e) Describe the stationary distributions for this graph.

Solution. There are infinitely many, with $d(b) = d(c) = 0$, and $d(a) = p$ and $d(d) = 1 - p$ for any p. ■

(f) If you start at node b and take a long random walk, the probability you are at node d will be close to what fraction? Explain.

Solution. $1/3$. ■

Appendix

A *random-walk graph* is a digraph such that each edge, $x \to y$, is labelled with a number, $p(x, y) > 0$, which will indicate the probability of following that edge starting at vertex x. Formally, we simply require that the sum of labels leaving each vertex is 1. That is, if we define for each vertex, x,

$$\text{out}(x) ::= \{y \mid x \to y \text{ is an edge of the graph}\},$$

then

$$\sum_{y \in \text{out}(x)} p(x, y) = 1.$$

A *distribution*, d, is a labelling of each vertex, x, with a number, $d(x) \geq 0$, which will indicate the probability of being at x. Formally, we simply require that the sum of all the vertex labels is 1, that is,

$$\sum_{x \in V} d(x) = 1,$$

where V is the set of vertices.

The distribution, $\widehat{d}$, *after a single step* of a random walk from distribution, d, is given by

$$\widehat{d}(x) ::= \sum_{y \in \text{in}(x)} d(y) \cdot p(y, x),$$

where

$$\text{in}(x) ::= \{y \mid y \to x \text{ is an edge of the graph}\}.$$

A distribution d is *stationary* if $\widehat{d} = d$, where $\widehat{d}$ is the distribution after a single step of a random walk starting from d. In other words, d stationary implies

$$d(x) ::= \sum_{y \in \text{in}(x)} d(y) \cdot p(y, x).$$

6.042J / 18.062J Mathematics for Computer Science
Spring 2010