ECS 20 (Spring 2013) – Phillip Rogaway – Lecture 1

Today:

- Introductory comments
- Some example problems

Announcements

- course information sheet online (from my personal homepage: 'Rogaway')
- first HW due Wednesday
- PS1, PS2, Q1 mandatory
- Introduce TAs: Darren, Theo

Topics of this class

- Discrete (not discreet!) mathematics deals with finite and countably infinite sets
- A term rarely used by mathematicians, who say what they do more specifically.
- Some branches mathematics that fall in scope of discrete math:
  - Combinatorics (how to count things, how to make combinatorial objects that have desired properties)
  - Graph theory (points and two-elements subsets of them)
  - Logic
  - Set theory (normally dealt with in a class like this, but much modern set theory is *not* dealing with finite or countably infinite sets)
  - Probability (again, routinely treated in discrete math classes, but only when we assume that the underlying "probability space" is finite or countably infinite).
  - And much more

Omit: meld into examples -- Helpful Techniques for Solving Discrete Math Problems

1. Generalize the problem (in the right way!)
2. Introduce variables (e.g., substituting n for 100 in Ex. 0)
3. Group terms cleverly (e.g., the algebraic analysis of Ex. 0)
4. Name the things that you are interested in.
5. Think recursively.
6. Solve small cases by hand and look for emerging patterns.
7. Substitute repeatedly to simplify "recurrence relations".
8. Use contradiction (this is demonstrated in Ex. 2).
9. Follow your nose (often only one natural path to go down) (eg, Ex. 2)

Some Example Problems

Example 1: Sum of the first *n* numbers

Find the following sum:

$$1 + 2 + \ldots + 100$$

or more generally

$$1 + 2 + \ldots + n$$

Gauss is said to have done this in seconds as a young child.

Solution:

This problem can be viewed algebraically by writing the list of numbers forwards and backwards, i.e.

$$\begin{array}{rl} & 1 + 2 + \ldots + (n-1) + n \\ + & n + (n-1) + \ldots + 2 + 1 \\ \hline & (n+1) + (n+1) + \ldots + (n+1) + (n+1) \end{array}$$

so $n(n+1)$

Since this result is really twice the sum we are looking for it follows that

$$1 + 2 + \ldots + n = (n\,(n+1)) / 2$$

Sums like this come up often so have their own notation that you will have seen,

$$\sum_{i=1}^{n} i$$

You can discover formulas like this by *induction*, which we will be doing much more of later.

This example can also be solved geometrically by writing twice 1 + 2 + … + n points in the following way:

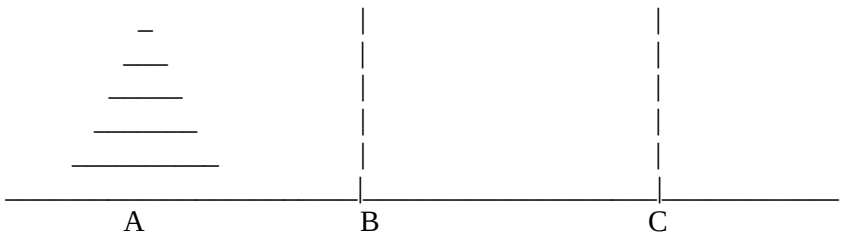
```
*   o   o   o   o
*   *   o   o   o
*   *   *   o   o      n points   (n=5 in the picture)
*   *   *   *   o
*   *   *   *   *
```

n + 1 points (n=5 in the picture)

So he total number of * points is

$(n^2 - n)/2 + n = n^2/2 + n/2 = n(n+1)/2$ which is the sum we are after.

Example 2: The Towers of Hanoi



Five rings of increasing diameter are placed on peg A. The pegs must be moved from A to C using the following rules:

- Only the topmost ring on a peg can be moved.
- A bigger ring cannot be placed on a smaller one.

Problem: Find a function that describes the least number of moves needed to solve the problem when you have n rings.

How many moves do you think it takes to move the five rings? Nobody guessed it or figured it out. Rogaway claims that the answer is 31.

We want a formula that specifies a number of moves that is both:

- **Sufficient**: there **is** a solution to the game using this number of moves.
- **Necessary**: no solution can use **fewer** moves than this.

Solution:

First, let's define what we're interested in. Let

T_n = The minimum number of moves needed to move the n rings from peg A to peg C (obeying the rules of the game).

Actually, this isn't good. We need to generalize the definition to do the job. So, instead, let

T_n = The minimum number of moves needed to move n rings from some one specified peg to some other specified peg (obeying the rules of the game).

Sufficiency:

Think recursively. Assume a "black box" algorithm can move the first n - 1 rings from any peg to any other peg. Solving the problem this way requires that the first n -1 rings be moved, then the largest ring be moved once, then the smaller rings be moved on to the largest ring. This number of moves can be represented by:

$$T_n \leq T_{n-1} + 1 + T_{n-1} = 2T_{n-1} + 1$$

Necessity:

Now we have to reason about *any* algorithm that solves the puzzle.
Any solution must move the largest ring to the final peg for the very last time. That takes one move. But before that happened, we had to get the n-1 rings that were formerly on top of the start peg and move them off to a free peg. That takes at least T_{n-1} moves. After we got the biggest ring to its destination peg, we had to move the n-1 smaller rings from the free peg where they were at to the final peg. That takes at least T_{n-1} moves. So, all in all, any solution needs to spend at least

$$T_n \geq 1 + T_{n-1} + T_{n-1} = 2T_{n-1} + 1$$

moves.

Putting together the two inequalities we have that

$$T_n = 2T_{n-1} + 1$$

We know that in order to move zero rings to their final location requires zero moves, so

$$T_0 = 0$$

Using this as our base value we can then determine that:

T_1	T_2	T_3	T_4	T_5	…	T_n	
1	3	7	15	31		$2^n - 1$	(apparently)

One way to get the general formula is by repeated substitution:

$$T_n = 2\,T_{n-1} + 1$$
$$= 2\,[2\,T_{n-2} + 1] + 1 = 2^2\,T_{n-2} + (1 + 2)$$
$$= 2^2\,[2\,T_{n-3} + 1] + (1 + 2) = 2^3\,T_{n-3} + (1 + 2 + 4)$$

$$= 2^n * 0 + (1 + 2 + 2^2 + \ldots + 2^{n-1})$$
$$= (1 + 2 + 2^2 + \ldots + 2^{n-1}) = 2^n - 1$$

Binary Representation

Example 3: Sqrt(2) is irrational

Prove that $x = \sqrt{2}$ is **irrational**.

Definition:

$x \in \mathbf{R}$ is **rational** if $x = p/q$ for some integers p and $q \in \mathbf{Z}$, $q \neq 0$.

$x \in \mathbf{R}$ is **irrational** if it is not rational.

Note: "if" in definitions mean "if and only if", or "exactly when"

Here we prove by contradiction.
Assume for contradiction that x *is* rational, ie,

$x = p/q$ for some integers p and q, $q \neq 0$

Without a loss of generality, it can be assumed that either p is odd or q is odd
(if they're both even, cross out the common factors of 2 until one of the numbers is odd).
Additionally, an odd number squared is still an odd number.

$\sqrt{2} = p/q$ square both sides:
$\rightarrow \quad 2 = p^2/q^2$ multiply through by the denominator:
$\rightarrow \quad 2q^2 = p^2$

From this we know that p is even, because the square of an odd number is odd (why?!). But then q is odd, because we know that at least one of p and q is odd. So we can write

$p = 2j$ for some $j \in \mathbf{Z}$ and

$q = 2i + 1$ for some $i \in \mathbf{Z}$

$\rightarrow 2(2i + 1)^2 = (2j)^2$

$\rightarrow (2i + 1)^2 = 2j^2$

$\rightarrow 4i^2 + 4i + 1 = 2j^2$

$\rightarrow 4(i^2 + i) + 1 = 2j^2$ $\rightarrow\leftarrow$

The contradiction is that an odd number (the LHS) can equal an even number (the RHS). We can conclude that our original assumption is wrong: $x = \sqrt{2}$ is **not** rational, which, by definition, means that it is **irrational**.

Example 4: Shuffling a deck of cards

Famous result (1992) of Bayer and Diaconis: In 1992, Bayer and Diaconis showed that after seven random riffle shuffles of a deck of 52 cards, every configuration is nearly equally likely.

TABLE 1
Total variation distance for m shuffles of 52 cards

m	1	2	3	4	5	6	7	8	9	10
$\|Q^m - U\|$	1.000	1.000	1.000	1.000	0.924	0.614	0.334	0.167	0.085	0.043

In gener, BD show that you need $1.5 \lg n + \Theta$ shuffes necessary and sufficient

Shuffling more than this does not significantly increase the "randomness"; shuffle less than this and the deck is "far" from random.
We claim that : 5 shuffles of a deck of cards is **not** enough to randomize the cards.

Here by **shuffles** I mean the usual "rifle shuffle." Prof. Rogaway demonstrates one with an imaginary deck.

Assume a starting sequence of

1, 2, 3, …, 51, 52

Even though we won't define what it means to randomize the cards, clearly a deck cannot be well randomized unless you can get **any** resulting sequence of cards, including, for example, the sequence:

52, 51, …, 3, 2, 1

We are going to show that 5 shuffles of this deck will **never** transform the specified starting sequence to the specified final sequence. So it can't do a good job of mixing the deck.

From http://www.math.hmc.edu/funfacts/ffiles/20001.4-6.shtml:

An amazing fact is that five random riffle shuffles are not enough to randomize a deck of cards, because not only is every configuration not nearly equally likely, there are in fact some configurations which are *not reachable* in 5 shuffles!

To see this, suppose (before shuffling) the cards in a deck are arranged in order from 1 to 52, top to bottom. After doing one shuffle, what kind of sequences are possible? A moment's reflection reveals that only configurations with 2 or fewer **rising sequences** are possible. A rising sequence is a maximal increasing sequential ordering of cards that appear in the deck (with other cards possibly interspersed) as you run through the cards from top to bottom. For instance, in an 8 card deck, 12345678 is the ordered deck and it has 1 rising sequence. After one shuffle,

16237845

is a possible configuration; note that it has 2 rising sequences (the black numerals form one, the red numerals form the other). Clearly the rising sequences are formed when the deck is cut before they are interleaved in the shuffle.

So, after doing 2 shuffles, how many rising sequences can we expect? At most 4, since each of the 2 rising sequences from the first shuffle have a chance of being cut in the second shuffle. So the number of rising sequences can at most double during each shuffle. After doing 5 shuffles, there at most 32 rising sequences.

But the *reversed* deck, numbered 52 down to 1, has 52 rising sequences! Therefore the reversed deck cannot be obtained in 5 random riffle shuffles!

Max number of rising sequences after

0 shuffles: 1
1 shuffles: 2
2 shuffles: 4
3 shuffles: 8
4 shuffles: 16
5 shuffles: 32 ← We still can't have reached anything with more than 32 rising sequences
6 shuffles: 52