CSC236 winter 2020

theory of computation

Colin Morris
colin@cs.toronto.edu

http://www.~~teach~~.cs.toronto.edu/~colin/236/W20/

Help yourselves to course info sheet

January 6, 2020

Outline

What is this course?

P'(n): Every bipartite graph on n vertices has no more than $n^2/4$ edges if n is even, or $(n^2-1)/4$ edges if n is odd.

base case: An empty bipartite graph has 0 vertices and 0 edges, and $0 \leq 0^2/4$, which verifies $P(0)$.

inductive step: Let n be an arbitrary, fixed, natural number. Assume $P'(n)$, that every bipartite graph on n vertices has no more than $n^2/4$ edges if n is even, or $(n^2-1)/4$ edges if n is even. I will show that $P'(n+1)$ follows, that every bipartite graph on $n+1$ edges has no more than $(n+1)^2/4$ edges if $n+1$ is even, or $[(n+1)^2-1]/4$ edges if $n+1$ is odd.
Let G be an arbitrary bipartite graph on $n+1$ vertices. Remove a vertex, together with its edges, from G's larger partition to produce a new bipartite graph G'. There are two possibilities, depending on whether $n+1$ is even or odd:

case $n+1$ is odd: G's smaller partition has, at most, $n/2$ vertices, so we removed at most $n/2$ edges to produce G'. $n+1$ odd means n is even, so by assumption $P(n)$, G' has at most $n^2/4$ edges, so accounting for the edges removed G had, at most:

$$\frac{n^2}{4} + \frac{n}{2} = \frac{n^2+2n}{4} \leq \frac{(n+1)^2-1}{4}$$

So $P'(n+1)$ follows in this case.

case $n+1$ is even: G's smaller partition has, at most, $(n+1)/2$ vertices, so we removed at most $(n+1)/2$ edges to produce G'. $n+1$ even means n is odd, so by assumption $P(n)$ G' has at most $(n^2-1)/4$ edges, so accounting for the edges removed G had, at most:

$$\frac{n^2-1}{4} + \frac{n+1}{2} = \frac{n^2+2n+1}{4} \leq \frac{(n+1)^2}{4}$$

So $P'(n+1)$ follows in this case.

$P'(n+1)$ follows in both possible cases ■

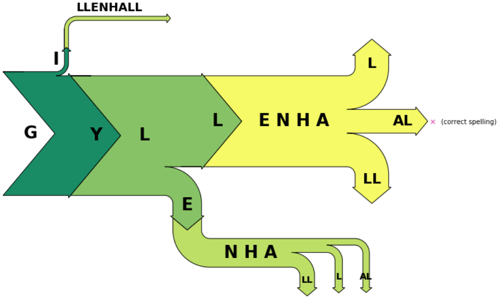
```
    try:
        f = codecs.open(filename, "r", encoding='UTF-8')
        lines = joinLines(f.readlines())
        f.close()
    except:
        pprint("Cannot read file: %s" % filename, sys.stderr)
        sys.exit(-2)

    return lines


def scan_for_selected_frames(lines):
    """scans for frames that should be rendered exclusively, 
true if such frames have been found"""
    p = re.compile("^!====\s*(.*?)\s*====(.*)", re.VERBOSE)
    for line in lines:
        mo = p.match(line)
        if mo is not None:
            return True
    return False

def line_opens_unselected_frame(line):
    p = re.compile("^====\s*(.*?)\s*====(.*)", re.VERBOSE)
    if p.match(line) is not None:
        return True
    return False

def line_opens_selected_frame(line):
```

More like this...

...than this

Who am I?

Computer Science
UNIVERSITY OF TORONTO



WIKIPEDIA
The Free Encyclopedia

myfavouritethings.jpg

Who are you?

Course information sheet

- Info is a subset of what's on the course website
- Let's take a tour now
  - (Sorry, this part is boring.)

About these slides

- Adapted from Danny Heap
- Plain slides posted online in advance
- Annotated slides uploaded after lecture
  - You may want to annotate your own copy during lecture

We behave as though you already know...

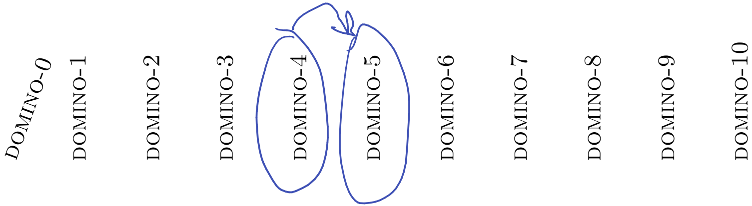
- CSC165 material, especially proofs and big-Oh material
  - But you can *relax* the structure a little
- Chapter 0 material from *Introduction to Theory of Computation*
- recursion, efficiency material from CSC148

By end of course you'll know...

1. Several flavours of proof by induction
2. Reasoning about recurrences
3. Proving the correctness of programs
4. Formal languages

Simple induction

Domino fates foretold



$$[\, P(0) \;\wedge\; (\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1)\,)\,] \Longrightarrow \forall n \in \mathbb{N}, P(n)$$

If the initial case works,
and each case that works implies its successor works,
then all cases work

Simple induction outline

Boolean function

$P(n)$: n is even

$\text{WTS: } \forall n \in \mathbb{N},\ P(n) \Rightarrow P(n+1)$

1. Define predicate, $P(n)$
2. Inductive step
   - 2.1 Let $n \in \mathbb{N}$
   - 2.2 Assume $P(n)$ (inductive hypothesis) I. H.
   - 2.3 use it to show that $P(n+1)$ holds

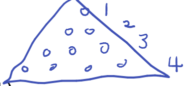
   I a miracle occurs here
3. Verify base case(s) (AKA basis)

   $P(0)$

4. (optional) conclusion

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

Example: triangular numbers



Show that for any n, $\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$.

1. Define predicate $P(n)$: $\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$

2. Inductive step Let $n \in \mathbb{N}$, assume $P(n)$

$$\sum_{k=0}^{n+1} k = \left(\sum_{k=0}^{n} k\right) + (\quad 1)$$

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

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

then $P(n+1)$

3. Base case

$$\sum_{k=0}^{0} k = 0 = \frac{0(0+1)}{2} \checkmark$$

so $P(0)$.

4. $\forall n \in \mathbb{N}, P(n)$.

Sometimes we need more than one base case

Show that $\forall n \in \mathbb{N}, 3^n \geq n^3$

$P(n)$: $3^n \geq n^3$

IS: Let $n \in \mathbb{N}$, assume $P(n) \wedge n \geq 3$

$$3^{n+1} = 3 \times 3^n$$

$$\geq 3 \times n^3 \quad \text{\# by IH.}$$

$$= n^3 + n^3 + n^3$$

$$\geq n^3 + 3n^2 + n^3 \quad \text{\# } n \geq 3$$

$$\geq n^3 + 3n^2 + (n^2 + n^2 + n^2) \quad \text{\# } n \geq 3$$

$$\geq n^3 + 3n^2 + n^2 + n^2$$

$$\geq n^3 + 3n^2 + 3n + 1 \quad \text{\# } n \geq 3$$

$$= (n+1)^3,$$

so $P(n+1)$

$$\geq (n+1)^3 = n^3 + 3n^2 + 3n + 1$$

Basis: $P(0) \wedge P(1) \wedge P(2) \wedge P(3)$

$3^3 = 27 \geq 27 = 3^3$, $P(3)$

$3^2 = 9 \geq 8 = 2^3$, $P(2)$

$3^1 = 3 \geq 1 = 1^3$, $P(1)$

$3^0 = 1 \geq 0 = 0^3$, $P(0)$

~~Sometimes we need more than one base case~~

~~Show that $\forall n \in \mathbb{N}, 3^n \geq n^3$~~

Welcome back to CSC 236

Reminders

- office hours after lecture @ BA2283
- tut rooms posted on website
  - please attempt exercises before Friday
- extra course info sheets available at the front.

Bases other than zero

Prove that $n! \geq n^2$ for $n >$???

n	$n!$	n^2	$n! \geq n^2$
0	1	0	✓
1	1	1	✓
2	2	4	✗
3	6	9	✗
4	24	16	✓
5	120	25	✓

Bases other than zero

Prove that $n! \geq n^2$ for $n > \cancel{???}$ 3

$P(n)$: $n! \geq n^2$

I.S. Let $n \in \mathbb{N}$, assume $n > 3 \wedge P(n)$

$(n+1)! = n!\,(n+1)$

$\geq n^2(n+1) = n^3 + n^2$

$> n^3 + 3n$ # $n > 3$

$= n^3 + 2n + n$

$\geq n^2 + 2n + 1$ # $n \geq 1$, $n^3 \geq n^2$

$= (n+1)^2$

$P(n+1)$

Basis

$4! = 24 \geq 16 = 4^2$, so $P(4)$

$\forall n \in \mathbb{N},\ n \geq 4 \Rightarrow P(n)$

[Conclusion, based on I.S. + Basis]

The units digit of any power of 7 is one of 1, 3, 7, or 9

Scratch work

n	units(n)
1	1
7	7
49	9
343	3
???	1

$$\begin{array}{r} \overset{2}{34}3 \\ \times \quad 7 \\ \hline 1 \end{array}$$

$P(n) = 7^n \equiv 1 \mod 10$

$\lor\ 7^n \equiv 3 \mod 10$

etc.

The units digit of any power of 7 is one of 1, 3, 7, or 9

Use the simple induction outline

let $U = \{1, 3, 7,$

$P(n)$: units digit of n is in U

$P(n)$: n is a power of 7 and its units digit is in U

[Context: these are predicates which we might be tempted to use here. However, they don't have the property that $P(n) \Rightarrow P(n+1)$, so they only work if we were to do a weird version of proof by induction. The proof on the next slide is the recommended way to go.

IS. Let $n \in \mathbb{N}$, assume $P(n)$

$P(7)$

$\Downarrow$

$P(49)$

...

then $P(7n)$

$P(1) \wedge \forall n \in \mathbb{N},\ P(n) \Rightarrow P(7n)$

thus

The units digit of any power of 7 is one of 1, 3, 7, or 9

Use the simple induction outline

let $U = \{1, 3, 7, 9\}$

$P(n)$: units digit of $7^n \in U$

Basis

$7^0 = 1$, units digit of 1 is 1, and $1 \in U$

IS Let $n \in \mathbb{N}$, assume $P(n)$

Case 1: units digit of 7^n is 1.

then units digit of $7^{n+1} = 7$

$7^{n+1} = 7 \times 7^n$, and the units digit of 7^n is 1, so 7^{n+1} units digit is 7.

Case 2: 7^n units digit is 3

Case 3

Case 4

etc.

$P(n+1)$

please don't be this lazy when writing your proofs. :)

The units digit of any power of 7 is one of 1, 3, 7, or 9

Use the simple induction outline

Let $U = \{1, 3, 7, 9, 2\}$

[Context: our failed attempt to modify prev proof, for version where 2 is among possible digits

$P(n)$: units digit of $7^n \in U$

Basis

$7^0 = 1$, units digit of 1 is 1, and $1 \in U$

IS

Let $n \in \mathbb{N}$, assume $P(n)$

Case 1: units digit of 7^n is 1.

then units digit of 7^{n+1}.

$7^{n+1} = 7 \times 7^n$, and the units digit of 7^n is 1, so 7^{n+1} units digit is 7.

Case 2: 7^n units digit is 3

Case 3

etc.

Case 4

$P(n+1)$

Case 5: $7^n = 10k + 2$, for some k

$7^{n+1} = 7(10k + 2)$

$= 70k + 14$

$= 10 \times (8k) + 4$

The units digit of any power of 7 is one of 1, **2**, 3, 7, or 9

Is the claim still true? What happens if you add this other case to the inductive step?

$Q(n)$: units of 7^n is in $\{1, 2, 3, 7, 9\}$

strengthening the I.H.

define $P(n)$ as before

prove $\forall n \; P(n)$ by induction

observe $P(n) \Rightarrow Q(n)$

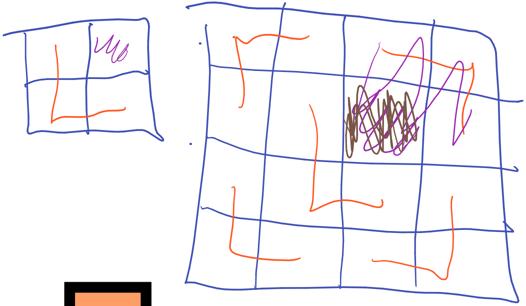
Extra exercise

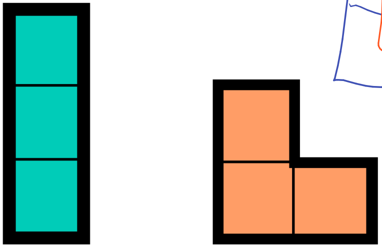
$$\frac{1}{1} + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} \cdots$$

$P(n)$: $\sum_{k=1}^{n} \frac{1}{k^2} < 2$ ← Can be proven via induction, but only if we strengthen our predicate.

Trominoes

See https://en.wikipedia.org/wiki/Tromino

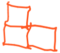




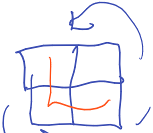
Can a $2^n \times 2^n$ square grid, **with one subsquare removed**, be tiled (covered without overlapping) by "chair" trominoes?

Trominoes

arbitrary

$P(n)$: a $2^n \times 2^n$ square grid with a subsquare removed can be tiled with chair  trominoes.

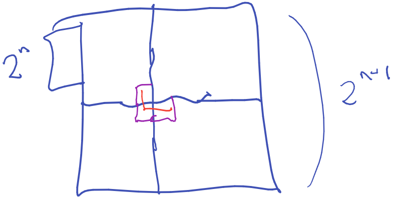
Basis

a 2×2 grid can be tiled minus 1 square:  , $P(1)$

a 1×1 grid can be tiled - 1 square like so:  , $P(0)$

I.S. Let $n \in \mathbb{N}$, assume $P(n)$

Consider a $2^{n+1} \times 2^{n+1}$ grid



... thus $P(n+1)$

Trominoes

$P(n)$: a $2^n \times 2^n$ square grid with a subsquare removed can be tiled with chair trominoes.

Note: we didn't finish this problem in lecture, though we found a good general approach for the inductive step (divide the 2^{n+1}x2^{n+1} grid into 4 subgrids, so we can apply the induction hypothesis.

We noted that the predicate as originally written was ambiguous, with a potential "weak" interpretation (the grid can be tiled with some square missing) vs. a "strong" one (the grid can be tiled with any *arbitrary* square missing). I claimed that it's possible to prove either version directly via induction. It's important that we don't exploit this ambiguity by assuming the strong version in our IH and then only proving the weak version for n+1!

Open question: once we fill in the inductive step, will it allow us to go from P(0) to P(1)? If not, that probably means we've made some implicit assumption about the n in our IH (which we should make explicit)