CSC 236 WINTER 2011 — WEEK 1

GARY BAUMGARTNER

Consider the following algorithm:

```
a = 1/5
while true
  print a
  a = (1 + a) / 2
```

What can we say about what it prints?

Heuristic: trace algorithms, code, sequences, proofs, statements, etc — make a table

- help us understand, especially what's going on inductively
- catch boundary off-by-one errors

output
1/5
3/5
4/5
9/10
19/20

Some conjectures about the sequence of displayed values:

- all less than one
- increasing
- limit is 1 — outside the scope of 236

Let's try to prove that they are all less than one.

Heuristic: convince ourselves

- proofs are simply (!) convincing summaries for experienced readers

Reasoning:

(1) a starts off less than one
(2) if a is less than 1 then replacing it with the average $\frac{1+a}{2}$, which is between a and 1, gives a new value still less than 1
(3) So, because
  (a) it is less than one at the start, and
  (b) each step preserves this,
  (c) it is always less than one.

To an experienced Computer Scientist or Mathematician, (1) & (2) is a complete proof, because they

- can do the algebra of (2)
- know the *Inductive Principle* (3):
  - The property is true at the start, and
  - each step preserves the truth of the property, so
  - the property is always true.

Let's contrast this with a justification that the sequence of values is increasing: is a always less than its replacement $\frac{1+a}{2}$, the average of a and one? Yes, because we convinced ourselves that a is always less than one, so the average of a and one is more than a. This doesn't require inductive reasoning (except that it relies on the previous result which did).

To study the difference between the two proofs more carefully, and help us reason about programs/algorithms in general, we get more formal.

In Java, Python and many (but not all: see CSC 324) computer languages:

- variables can have which value they contain change
- values can refer to objects, and those objects can change themselves

[Review 108 if the difference between variables and values in code is in any way unclear to you]

Mathematical variables don't vary: they represent a fixed but possibly unknown value. This makes things simpler! To reason about CS variables mathematically, we index their values.

For $n \in \mathbb{N}$, let a_n be the value of a after n iterations. In particular, a_0 means the initial value of a.

Heuristic: express ourselves symbolically

[Review 165 if this gives you any trouble at all]

Our two claims are now:

$$\forall n \in \mathbb{N}, a_n < 1$$
$$\forall n \in \mathbb{N}, a_n < a_{n+1}$$

Our sequence is defined by:

$$\begin{aligned} a_0 &= \frac{1}{5} \\ a_{n+1} &= \frac{1+a_n}{2}, \text{ for all } n \in \mathbb{N} \end{aligned}$$

Exercise: trace the claims and the sequence, for the reasons we stated above (in lecture we caught an off-by-one error)

Now we formalize our justification of the two claims.

Proof. $a_0 = \frac{1}{5} < 1$

Let $n \in \mathbb{N}$, and suppose $a_n < 1$.

Then $a_{n+1} = \frac{1+a_n}{2} < \frac{1+1}{2} = 1$.

Therefore $\forall n \in \mathbb{N}, a_n < 1$. □

Proof. Let $n \in \mathbb{N}$.

From above, $a_n < 1$.

So $a_{n+1} = \frac{1+a_n}{2} > \frac{a_n+a_n}{2} = a_n$.

Therefore $\forall n \in \mathbb{N}, a_n < a_{n+1}$. □

The second proof is a standard direct proof of its conclusion.

But the first proof shows that

$$a_0 < 1 \wedge \forall n \in \mathbb{N}, a_n < 1 \to a_{n+1} < 1$$

and concludes that

$$\forall n \in \mathbb{N}, a_n < 1.$$

So it is implicitly using the Inductive Principle

$$\left[a_0 < 1 \wedge \forall n \in \mathbb{N}, a_n < 1 \to a_{n+1} < 1\right] \to \left[\forall n \in \mathbb{N}, a_n < 1\right].$$

This principle works in general: let P be a predicate with domain $\mathbb{N}$, then

$$\left[P(0) \wedge \forall n \in \mathbb{N}, P(n) \to P(n+1)\right] \to \left[\forall n \in \mathbb{N}, P(n)\right].$$

Since we all (?) believe this principle, we can prove $\forall n \in \mathbb{N}, P(n)$ by instead proving $P(0) \wedge \forall n \in \mathbb{N}, P(n) \to P(n+1)$. This is the *technique* that follows from the *Principle* of Induction.

[165 Review: put in all implicit parentheses in our symbolic statements, and define the specific P's we studied. Be sure that your P's are boolean and open in a single natural number, by writing out $P(236)$ via textual substitution (I/we did this in lecture, and caught some problems).]

There is a common style for writing up proofs that follow the above principle:

Proof. By Induction.

Base Case ... thus $P(0)$.

Inductive Step Let $n \in \mathbb{N}$. Suppose $P(n)$ (IH). ["IH" stands for "Inductive Hypothesis"]

... [use $P(n)$, aka "IH", to help fill in the blank — if we didn't use it, we rewrite the proof directly (without induction)]

Thus $P(n+1)$. □

Exercise: write up our inductive proof in this style.

Let's reflect on when to try using Induction.

Heuristic: When we *have* a connection between nth and $n+1$st (the definition of the example sequence was inductive, connecting a_n and a_{n+1}) and want to *show* something *without* such a connection (e.g. $a_n < 1$), try the Principle of Induction above. But to *show* something that connects nth and $n+1$st, try a direct proof (first).

Making A Problem Inductive

Let's prove that $12^n - 1$ is divisible by 11 for each $n \in \mathbb{N}$. To practice:

n	$12^n - 1$	As $11 \cdot \_\_$
0	$1 - 1 = 0$	$11 \cdot 0$
1	$12 - 1 = 11$	$11 \cdot 1$
2	$144 - 1 = 143$	$11 \cdot 13$
3	?	?

The sequence $a_n = 12^n - 1$ isn't given inductively. To use Induction to reason about it, we want it inductive. One approach is to notice that it's almost 12^n, which is inductive. So let's go from $12^n - 1$ to 12^n to 12^{n+1} to $12^{n+1} - 1$:

$$12^{n+1} - 1 = 12 \cdot [(12^n - 1) + 1] - 1$$

Exercise: use this to fill in the 3rd row of the table.

We're viewing the sequence now as

$$\begin{aligned} a_0 &= 0, \\ a_{n+1} &= 12 \cdot [a_n + 1] - 1, \text{ for } n \in \mathbb{N} \end{aligned}$$

Exercises: sanity check, write in terms of n vs. $n-1$, write the corresponding iterative and recursive programs.

So if $a_n = 11k$ then $a_{n+1} = 12[11k+1] - 1 = 12 \cdot 11k + 12 - 1 = 11 \cdot (12k+1)$. So we're convinced, by the same Inductive Principle as above. P here is defined as: for $n \in \mathbb{N}$, $P(n)$ is $\exists k \in \mathbb{N}, 12^n - 1 = 11k$. Now we can give a careful proof.

Proof. By Induction.

Base Case: 0 $12^0 - 1 = 1 - 1 = 0 = 11 \cdot 0$.

Inductive Step Let $n \in \mathbb{N}$. Suppose $12^n - 1 = 11k$ for some $k \in \mathbb{N}$ (IH).

$$\begin{aligned} \text{Then} \quad 12^{n+1} - 1 &= 12 \cdot 12^n - 1 \\ &= 12 \cdot [(12^n - 1) + 1] - 1 \\ &= 12 \cdot [11k + 1] - 1 \text{ by (IH)} \\ &= 12 \cdot 11k + 12 - 1 \\ &= 12 \cdot 11k + 11 \\ &= 11(12k + 1), \text{ where } 12k + 1 \in \mathbb{N} \text{ since } k \in \mathbb{N}. \end{aligned}$$

□

There are actually two results hiding in the above proof: that the inductive definition of a_n above matches the original definition as $12^n - 1$, and that the inductively defined a_n's are divisible by 11.

Exercise: write out each proof separately.

Exercise: some students suggested viewing a_n as

$$\begin{aligned} a_0 &= 0, \\ a_{n+1} &= 12 \cdot a_n + 11, \text{ for } n \in \mathbb{N} \end{aligned}$$

Repeat our work above using this approach.