EECS/MATH 1019
Section 5.2: Strong Induction (continued)
Section 5.3: Recursion and Structural Induction

February 28, 2023

Section 5.2: Strong Induction — Recall from February 16:

Let $P(1), P(2), P(3), \ldots$ be statements. Assume

(a') $P(1)$ is true, and

(b'') $[P(1) \wedge P(2) \wedge P(3) \wedge \ldots \wedge P(k)] \rightarrow P(k+1)$ for every $k \in \mathbb{Z}^+$.

Then $P(n)$ is true for every $n \in \mathbb{Z}^+$.

(Note: Assumption (b'') says that $P(1) \rightarrow P(2)$ and $[P(1) \wedge P(2)] \rightarrow P(3)$ and $[P(1) \wedge P(2) \wedge P(3)] \rightarrow P(4)$ and $\ldots$.)

Like ordinary induction, we can start at another integer besides 1. For example, we can use the following form:

Let $P(0), P(1), P(2), \ldots$ be statements. Assume

(a') $P(0)$ is true, and

(b'') $[P(0) \wedge P(1) \wedge P(2) \wedge \ldots \wedge P(k)] \rightarrow P(k+1)$ for every $k \in \mathbb{N}$.

Then $P(n)$ is true for every $n \in \mathbb{N}$.

Example 11: A game with piles of coins

Initially you have n coins in one pile (where $n \in \mathbb{Z}^+$).

The game has the following rule: Whenever you have a pile containing more than 1 coin, you can split that pile into two smaller piles. You repeat this process until you end up with n piles, each containing one coin.

During the game, you earn points. Each time you split a pile into two smaller piles, the number of points you earn equals the product of sizes of these two new piles. You then add up all the points that you have earned for as long as the game lasts.

For example, if you start with a pile of 10 coins, you could split it into one pile of 3 coins and another pile of 7 coins, earning 3×7 points (i.e., 21 points). Then you could split the pile of 7 into one pile of 6 and another pile of 1, earning another 6×1 points. This gives you $21 + 6$ points so far, but you still have piles to split, which will give you more points.

For example, suppose n is 6.

Start with one pile of 6:	6	Points
Split 6 into 4 and 2:	$\overbrace{4,\quad 2}$	$4 \times 2 = 8$
Split 4 into 1 and 3:	$\overbrace{1,\quad 3},\quad 2$	$1 \times 3 = 3$
Split 3 into 2 and 1:	$1,\quad \overbrace{2,\quad 1},\quad 2$	$2 \times 1 = 2$
Split first 2 into 1 and 1:	$1,\quad \overbrace{1,\quad 1},\quad 1,\quad 2$	$1 \times 1 = 1$
Split last 2 into 1 and 1:	$1,\quad 1,\quad 1,\quad 1,\quad \overbrace{1,\quad 1}$	$1 \times 1 = 1$

Total points: $8 + 3 + 2 + 1 + 1 = 15$.

Try another strategy:	6	Points
Split 6 into 3 and 3:	$\overbrace{3,\quad 3}$	$3 \times 3 = 9$
Split first 3 into 1 and 2:	$\overbrace{1,\quad 2},\quad 3$	$1 \times 2 = 2$
Split 3 into 1 and 2:	$1,\quad 2,\quad \overbrace{1,\quad 2}$	$1 \times 2 = 2$
Split first 2 into 1 and 1:	$1,\quad \overbrace{1,\quad 1},\quad 1,\quad 2$	$1 \times 1 = 1$
Split last 2 into 1 and 1:	$1,\quad 1,\quad 1,\quad 1,\quad \overbrace{1,\quad 1}$	$1 \times 1 = 1$

Total points: $9 + 2 + 2 + 1 + 1 = 15$.

Is 15 the best we can do for 6 coins? Can we do any worse?

It turns out that we always get 15 points from 6 coins.

We shall use Strong Induction to prove that the total number of points will be $(n^2 - n)/2$, no matter how we decide split the piles at each step.

Proof: For every natural number n, let $P(n)$ be the statement

$P(n)$: For an initial pile of n coins, the game always results in exactly $(n^2 - n)/2$ points.

We want to use Strong Induction to prove that $P(n)$ is always true.

For $n = 1$: With only one coin, there is no split, and we get no points. This agrees with taking $n = 1$ in the formula $(n^2 - n)/2$, which gives 0. Therefore we have shown that $P(1)$ is true.

Now let $k \in \mathbb{Z}^+$ and assume that $P(1)$, $P(2)$,..., $P(k)$ are all true. We would like to deduce the $P(k+1)$ must also be true. Accordingly, suppose that you start with a pile of $k+1$ coins, and that you begin by splitting it into one pile of A coins and another pile of B coins, where $A + B = k + 1$ (and $A \geq 1$ and $B \geq 1$). Then A and B are both in the set $\{1, 2, \ldots, k\}$. In particular, this tells us that $P(A)$ and $P(B)$ are both true (by our inductive assumption).

You split the pile of $k+1$ into A and B $\quad (A+B = k+1)$

Now let's count your points. You get AB points from your first split, after which you have a pile of size A and another pile of size B. Since $P(A)$ is true, all of the splits you ever make in the coins in the pile of size A must produce $(A^2-A)/2$ points. Similarly, since $P(B)$ is true, all of the splits you ever make in the coins in the pile of size B must produce $(B^2-B)/2$ points. And that's all the points you get. So the total of all the points is

$$
\begin{aligned}
AB + \frac{A^2-A}{2} + \frac{B^2-B}{2} &= \frac{2AB + A^2 - A + B^2 - B}{2} \\
&= \frac{(A+B)^2 - (A+B)}{2} \\
&= \frac{(k+1)^2 - (k+1)}{2}.
\end{aligned}
$$

In particular, the total does not depend on your choice of A and B. Thus, any choice of splits always results in $[(k+1)^2-(k+1)]/2$ points, which shows that $P(k+1)$ is true.

Thus we have proved that $[P(1) \wedge P(2) \wedge \cdots P(k)] \rightarrow P(k+1)$ for every $k \in \mathbb{Z}^+$.

Therefore, by Strong Induction, it follows that $P(n)$ is true for every $n \in \mathbb{Z}^+$.

Section 5.3: Recursive Definitions

Recall Example 10 from class of February 16:

Let $a_1, a_2, a_3, \ldots$ be the sequence of real numbers defined by

$$a_1 = 1, \quad a_2 = 5, \quad \text{and} \quad a_{n+1} = a_n + 2a_{n-1} \quad \text{for } n = 2, 3, 4, \ldots$$

Then
$$\begin{aligned} a_3 &= a_2 + 2a_1 = 5 + 2(1) = 7, \\ a_4 &= a_3 + 2a_2 = 7 + 2(5) = 17, \\ a_5 &= a_4 + 2a_3 = 17 + 2(7) = 31, \end{aligned} \qquad \ldots \text{and so on.}$$

This is a *recursive* definition (also called an *inductive* definition). After some initial values are specified, each a_n is defined using other (previous) terms of the sequence.

<u>Remark:</u> Equivalently, instead of a sequence $a_1, a_2, a_3, \ldots$, we can define a function $A : \mathbb{Z}^+ \to \mathbb{R}$ recursively by

$$A(1) = 1, \quad A(2) = 5, \quad \text{and} \quad A(n+1) = A(n) + 2A(n-1) \quad \text{for } n = 2, 3, 4, \ldots$$

This function is identified with the above sequence by $A(n) = a_n$ for every $n \in \mathbb{Z}^+$. (Essentially the same.)

Summations can also be defined recursively.

E.g. Define the function $S : \mathbb{Z}^+ \to \mathbb{R}$ by

$$S(n) \;=\; \sum_{k=1}^{n} \frac{1}{k^2}\,.$$

That is, $\quad S(1) \;=\; \sum_{k=1}^{1} \frac{1}{k^2} \;=\; \frac{1}{1}, \quad S(2) \;=\; \sum_{k=1}^{2} \frac{1}{k^2} \;=\; \frac{1}{1} + \frac{1}{4},$

We can give a recursive definition of this function by

$$S(1) \;=\; 1 \quad \text{and} \quad S(n) \;=\; S(n-1) + \frac{1}{n^2} \;\; \text{for } n = 2, 3, \cdots$$

E.g. $\quad S(3) \;=\; S(2) + \frac{1}{9} \;=\; \frac{1}{1} + \frac{1}{4} + \frac{1}{9}\,; \qquad S(4) \;=\; S(3) + \frac{1}{16}\,.$

Another well known example of a recursive definition is the Fibonacci sequence

0	1	1	2	3	5	8	13	21	34	55	$\cdots$
f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	$\cdots$

This sequence is usually defined recursively:

$$f_0 = 0, \; f_1 = 1 \;, \text{and} \quad f_n = f_{n-1} + f_{n-2} \quad \text{for } n = 2, 3, \ldots .$$

The Fibonacci numbers have lots of interesting properties, many of which can be proved by induction. See the Exercises in Section 5.3 for some examples. Here is one:

Cassini's Formula: *$f_{n+1} f_{n-1} - f_n^2 = (-1)^n$ for every $n \geq 1$.*

E.g. $n = 1$: $f_2\, f_0 - f_1^2 = (1)(0) - 1^2 = -1 = (-1)^1$.

$n = 2$: $f_3\, f_1 - f_2^2 = (2)(1) - 1^2 = 1 = (-1)^2$.

$n = 3$: $f_4\, f_2 - f_3^2 = (3)(1) - 2^2 = 3 - 4 = -1 = (-1)^3$.

$n = 4$: $f_5\, f_3 - f_4^2 = (5)(2) - 3^2 = 10 - 9 = 1 = (-1)^4$.

$n = 9$: $f_{10}\, f_8 - f_9^2 = (55)(21) - 34^2 = 1155 - 1156 = (-1)^9$.

$f_{n+2} = f_{n+1} + f_n$ for $n = 0, 1, 2, \ldots$, and $f_0 = 0,\ f_1 = 1$.

Cassini's Formula: $f_{n+1}f_{n-1} - f_n^2 = (-1)^n$ *for every* $n \geq 1$.

Proof: Let $P(n)$ be the statement $f_{n+1}f_{n-1} - f_n^2 = (-1)^n$.
We checked that $\underline{P(1) \text{ is true}}$ (as well as $P(2)$, $P(3)$, $P(4)$, $P(9)$).

Assume $k \geq 1$ and $P(k)$ is true, i.e. $f_{k+1}f_{k-1} - f_k^2 = (-1)^k$.
Our goal is to derive $P(k+1)$. So we need to show that
$f_{k+2}f_k - f_{k+1}^2$ is equal to $(-1)^{k+1}$.

$$
\begin{aligned}
f_{k+2}f_k - f_{k+1}^2 &= (f_{k+1} + f_k)f_k - f_{k+1}^2 \\
&= f_{k+1}f_k + f_k^2 - f_{k+1}^2 \\
&= f_k^2 + f_{k+1}(f_k - f_{k+1}) \qquad \text{Now use } f_{k+1} = f_k + f_{k-1} : \\
&= f_k^2 + f_{k+1}(-f_{k-1}) \\
&= -(f_{k+1}f_{k-1} - f_k^2) \qquad \text{Now use } P(k): \\
&= -(-1)^k = (-1)^{k+1}.
\end{aligned}
$$

This gives $P(k+1)$. Therefore $\underline{P(k) \rightarrow P(k+1) \text{ for every } k \geq 1.}$
Therefore $P(n)$ is true for every $n \geq 1$ by mathematical induction.
Q.E.D.

Recursively Defined Sets and Structures (sec. 5.3.3)

Here is a way to define the set of positive integers recursively.
Let S be the subset of real numbers defined by

(i) *Basis step:* $1 \in S$.
(ii) *Recursive step:* If $x \in S$, then $x + 1 \in S$.
(iii) And S has no other elements.
(We will not bother to mention (iii) in future.)

Then S is the set of positive integers.

What is the set T that is defined by the following rules?

(i) *Basis step:* $1 \in T$.
(ii) *Recursive step:* If $x \in T$, then $x + 2 \in T$.

$1 \in T$, therefore $1 + 2 \in T$, i.e. $3 \in T$;
and therefore $3 + 2 \in T$, i.e. $5 \in T$;
and therefore $5 + 2 \in T$, i.e. $7 \in T$;
and so on ...

<u>Answer:</u> T is the set of odd positive integers.

Poll: What is the set V that is defined by the following rules?

(i) *Basis step:* $1 \in V$.

(ii) *Recursive step:* If $x \in V$, then $x + 2 \in V$ and $x - 2 \in V$.

(A) V is the set of all integers.
(B) V is the set of odd positive integers.
(C) V is the set of all odd integers.
(D) V is the set of odd integers m such that $m \geq -1$.

Answer: (C).

$1 \in V$; therefore taking $x = 1$ in step (ii), we see that
$1 + 2 \in V$ and $1 - 2 \in V$, i.e. $3 \in V$ and $-1 \in V$.

Now we can take x to be 3 or -1 in step (ii).
Taking $x = 3$ first, we see that
$3 + 2 \in V$ and $3 - 2 \in V$, i.e. $5 \in V$ and $1 \in V$;
taking $x = -1$ next, we see that
$-1 + 2 \in V$ and $-1 - 2 \in V$, i.e. $1 \in V$ and $-3 \in V$.

Now the new possibilities for x are 5 and -3.
So V contains $5 + 2$, $5 - 2$, $-3 + 2$, and $-3 - 2$.

Now the new possibilities for x are 7 and -5. And so on...

Here is one more example of a recursively defined set of integers.

(i) *Basis step:* $3 \in W$.
(ii) *Recursive step:* If $x \in W$, then $x + 12 \in V$ and $x - 4 \in W$.

$3 \in W$; therefore taking $x = 3$ in step (ii), we see that
$3 + 12 \in W$ and $3 - 4 \in W$, i.e. $15 \in W$ and $-1 \in W$.

Now we can take x to be 15 or -1 in step (ii).
Taking $x = 15$ first, we see that
$15 + 12 \in W$ and $15 - 4 \in W$, i.e. $27 \in W$ and $11 \in W$;
taking $x = -1$ next, we see that
$-1 + 12 \in W$ and $-1 - 4 \in W$, i.e. $11 \in W$ and $-5 \in W$.

Now the new possibilities for x are 27, 11 and -5.
So W contains $27 + 12$, $27 - 4$, $11 + 12$, $11 - 4$, $-5 + 12$ and $-5 - 4$.

Now the new possibilities for x are 39, 23, 7, and -9. And so on...

It may not be so clear yet exactly what the set W is. For example, is 1 an element of W? We shall soon introduce a method called *structural induction* that lets us prove some things about W.

Strings

Let Σ be a set (usually finite). A string over Σ is a finite sequence of elements of Σ. (Order matters!)

E.g. if $\Sigma = \{a, b, c, d\}$, then some strings over Σ are *abdba*, and *baadb*, and *cccacaac*, and *d*, and *aaa*.

The number of symbols in a string is its length.

We call Σ the alphabet, and we call its elements symbols or characters.

The empty string is a string with no symbols; we denote it by λ. The length of λ is 0.

If s and t are strings over Σ, then their concatenation st is the string obtained by writing t immediately to the right of s.

E.g. For $\Sigma = \{a, b, c, d\}$: Let $s = dabbd$ and $t = cca$.
Then $st = dabbdcca$ and $ts = ccadabbd$.

Also $sb = dabbdb$ and $s\lambda = dabbd$.

For any string w, we have $w\lambda = \lambda w = w$.

The set of all strings over Σ is denoted Σ^*. It is defined recursively by

(i) *Basis step:* $\lambda \in \Sigma^*$.

(ii) *Recursive step:* If $w \in \Sigma^*$ and $x \in \Sigma$, then $wx \in \Sigma^*$.

Example: For $\Sigma = \{a, b, c, d\}$, we see that Σ^* contains λa, λb, λc, and λd, which equal a, b, c, and d respectively.

Taking $w = a$, we see that Σ^* contains aa, ab, ac, and ad.

Taking $w = b$, we see that Σ^* contains ba, bb, bc, and bd.

Similarly, Σ^* contains ca, cb, cc, cd, da, db, dc, and dd.

Taking $w = aa$, we see that Σ^* contains aaa, aab, aac, and aad.

Taking $w = ab$, we see that Σ^* contains aba, abb, abc, and abd.

And so on...

Example: A binary string is a string over the alphabet $\{0, 1\}$. Then $\{0, 1\}^*$ is the set of all binary strings.

Example: Here is a recursive definition of a particular subset E of bit strings.
(i) *Basis step:* $\lambda \in E$.
(ii) *Recursive step:* If $w \in E$, then $w1 \in E$, $1w \in E$, and $0w0 \in E$.

So E contains λ, as well as the following strings:
(Taking w to be λ:) $\lambda 1$, 1λ, and $0\lambda 0$; that is, 1 and 00;
(Taking w to be 1:) 11, 11, and 010; that is, 11 and 010;
and
(taking w to be 00:) 001, 100, and 0000; that is, 001, 100, and 0000;
and so on. . .

Question: Is 10111101110 in E?
We shall return to this question in the next class.

Next class: We will conclude Section 5.3 and begin Section 8.1 (you omit subsections 5.3.5 and 8.1.3).

Homework reminders:

- Homework assignment 5 (in Connect) is due Sunday March 5.
- Problem Set B (in Crowdmark) is also due Sunday March 5.