Reasoning About Programs

Week 3 PMT - Mathematical and Strong Induction
To discuss during PMT - do NOT hand in

Sophia Drossopoulou and Mark Wheelhouse

Aims: to be able to apply the mathematical and strong induction principles to particular cases and to be able to decide when to use each variety of induction.

In the following, $\mathbb{N}$ stands for the natural numbers $\{0, 1, 2...\}$, $\mathbb{N}^+$ stands for the positive natural numbers $\{1, 2...\}$ and $\mathbb{Z}$ stands for the integers $\{..., -2, -1, 0, 1, 2, ...\}$.

In these exercises you will have to decide which form of induction to use.

1st Question:

If you are confident with the basics of mathematical induction, then I propose you skip this question

Consider the assertion:

$$(*) \quad \forall n \in \mathbb{N}. \sum_{i=0}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$$

(a) Write out the mathematical induction principle applied on the assertion from above.

(b) Prove $(*)$ by induction.

A possible answer:

(c) Let $P(n)$ be defined as $P(n) \equiv \sum_{i=0}^{n} i^2 = \frac{n}{6}(n+1)(2n+1)$.
The application of the mathematical induction principle gives

$\sum_{i=0}^{0} i^2 = \frac{0}{6}(0+1)(2*0+1)$
$\land$
$\forall k \in \mathbb{N}\, [\, \sum_{i=0}^{k} i^2 = \frac{k}{6}(k+1)(2*k+1) \ \to \sum_{i=0}^{k+1} i^2 = \frac{k+1}{6}(k+1+1)(2*(k+1)+1) \ \ ]$
$\longrightarrow$
$\forall n \in \mathbb{N}. \sum_{i=0}^{n} i^2 = \frac{n}{6}(n+1)(2n+1)$

We will prove $(*)$ by mathematical induction on n.

Base case:

To show: $\sum_{i=0}^{0} i^2 = \frac{0}{6}(0+1)(2*0+1)$

$$\begin{aligned}
&\textstyle\sum_{i=0}^{0} i^2 \\
&= 0 && \text{by def. of } \textstyle\sum \\
&= 0*1*1 && \text{by arithm. laws} \\
&= \tfrac{0}{6}(0+1)(2*0+1) && \text{by arithm laws}
\end{aligned}$$

Inductive Step:

Take an arbitrary $k \in \mathbb{N}$.
Inductive Hypothesis: $\sum_{i=0}^{k} i^2 = \frac{k}{6}(k+1)(2k+1)$
To show: $\sum_{i=0}^{k+1} i^2 = \frac{k+1}{6}((k+1)+1)(2(k+1)+1)$

$$
\begin{aligned}
&\textstyle\sum_{i=0}^{k+1} i^2 \\
&\quad = (k+1)^2 + \textstyle\sum_{i=0}^{k} i^2 && \text{by def. of } \textstyle\sum \\
&\quad = (k+1)^2 + \tfrac{k}{6}(k+1)(2k+1) && \text{by ind. hyp.} \\
&\quad = \tfrac{k+1}{6}(6(k+1) + k(2k+1)) && \text{by rearranging} \\
&\quad = \tfrac{k+1}{6}(2k^2 + 7k + 6) && \text{by rearranging} \\
&\quad = \tfrac{k+1}{6}(k+2)(2k+3) && \text{by rearranging} \\
&\quad = \tfrac{k+1}{6}(k+2)(2(k+1)+1) && \text{by rearranging} \\
&\quad = \tfrac{k+1}{6}((k+1)+1)(2(k+1)+1) && \text{by rearranging}
\end{aligned}
$$

2nd Question:

Consider the function `f` defined as:

```
f :: Int -> Int
f n = n^3 - 25 * n
```

(a) Apply the mathematical induction principle on $(*)$ $\forall n \in \mathbb{N}.\ \exists i \in \mathbb{Z}.\ \texttt{f}\ n = 6 * i$.

(b) Prove $(*)$.
Hint: You may need to use some further lemmas about when mathematical terms are multiples of 6. State and prove any such lemmas.

(c) Using the result from part (b), show, *without using induction*, that,
$\forall j \in \mathbb{Z}.\ \exists i \in \mathbb{Z}.\ \texttt{f}\ j = 6 * i$.
i.e. show that the result holds also for negative numbers.

(d) Describe in up to four sentences how you would prove *using induction*, that,
$\forall j \in \mathbb{Z}.\ \exists i \in \mathbb{Z}.\ \texttt{f}\ j = 6 * i$.

(e) Using the result from part (b), prove, by induction, that, for all $n \geq 0$, all elements of the list generated by `ff` n given below are divisible by 6:

```
ff :: Int -> [Int]
ff 0 = [0]
ff n =  f n : ff (n-1)
```

A possible answer:

(a) Let $P \subseteq \mathbb{N}$ be defined as $P(n) \equiv \exists i \in \mathbb{Z}.\ \texttt{f}\ n = 6 * i$.
The mathematical induction principle then gives:

$\exists i \in \mathbb{Z}.\ \texttt{f}\ 0 = 6 * i$
$\wedge$

$\forall k \in \mathbb{N}.\ [\ \exists i \in \mathbb{Z}.\ \texttt{f}\ \ k = 6 * i\ \ \rightarrow\ \ \exists i \in \mathbb{Z}.\ \texttt{f}\ \ (k+1) = 6 * i\ ]$
$\longrightarrow\ \ \forall n \in \mathbb{N}.\ \exists i \in \mathbb{Z}.\ \texttt{f}\ \ n = 6 * i$

(b) We prove $\forall n \in \mathbb{N}.\ P(n)$ by mathematical induction on n.

Base case:

To show: $\exists i \in \mathbb{Z}.\ \texttt{f}\ \ 0 = 6 * i$

$$\begin{array}{lll} \texttt{f}\ \ 0 & & \\ = & 0^3 - 25 * 0 & \text{by definition of } \texttt{f} \\ = & 0 & \text{by arithemtic} \\ = & 6 * 0 & \text{by arithmetic} \end{array}$$

Therefore, $\exists i \in \mathbb{Z}. 6 * i = \texttt{f}\ \ 0$.

Inductive Step:

Take an arbitrary $k \in \mathbb{N}$.
Inductive Hypothesis: $\exists m \in \mathbb{Z}.\ \texttt{f}\ \ k = 6 * m$
To show: $\exists i \in \mathbb{Z}.\ \texttt{f}\ \ (k+1) = 6 * i$

Proof idea: We will first manipulate the term $\texttt{f}\ \ (k+1)$, until we obtain an equivalent term which is of the from $(\texttt{f}\ \ k) + \mathit{some\_rest}$. We will then apply the inductive hypothesis on k and show that *some_rest* is also a multiple of 6.

We first prove the following facts:

(A): Choose $m1 \in \mathbb{Z}$ such that $\texttt{f}\ \ k = 6 * m1$. We know that such an $m1$ exists, because of the Inductive Hypothesis.[1]

(B): $\forall n \in \mathbb{N}.\ \exists i \in \mathbb{Z}.\ (3 * n^2 + 3n) - 24 = 6 * i$. We will prove **(B)** below.

(C): Choose $m2 \in \mathbb{Z}$ such that $3 * \texttt{f}\ \ k^2 + 3 * \texttt{f}\ \ k - 24 = 6 * m2$. We know that such an $m2$ exists, because of **(B)**.[2]

We now manipulate the term $\texttt{f}\ \ (k+1)$:

$$\begin{array}{llll} \texttt{f}\ \ (k+1) & = & (k+1)^3 - 25(k+1) & \text{by definition of } \texttt{f} \\ & = & k^3 + 3k^2 + 3k + 1 - 25k - 25 & \text{by rearranging} \\ & = & (k^3 - 25k) + (3k^2 + 3k - 24) & \text{by rearranging} \\ & = & (\texttt{f}\ \ k) + (3k^2 + 3k) - 24 & \text{by definition of } \texttt{f} \\ & = & 6 * m1 + 6 * m2 & \text{by } \textbf{(A)} \text{ and} \textbf{(C)}. \end{array}$$

Now, taking $m3 = m1 + m2$, we obtain from above that $\texttt{f}\ \ (k+1) = 6 * m3$. Therefore, $\exists i \in \mathbb{Z}.\ \texttt{f}\ \ (k+1) = 6 * i$ and we are done.

Proof of (B):

Take $j \in \mathbb{N}$, arbitrary.

We want to show $\quad (\alpha)\ \exists m : \mathbb{Z}. 3 * j^2 + 3 * j - 24 = 6 * m.$

We show this as follows:

(D): Chose an $i \in \mathbb{Z}$, such that $j^2 + j = 2 * i$.
We can justify **(D)** because $j^2 + j$ is even. Namely, if j is even, then $j = 2 * i1$ for some $i1 \in \mathbb{Z}$ and then the assertion follows by taking $i = i1 * (k+1)$. And if j is odd, then $j + 1$ is even, in which case $j + 1 = 2 * i2$ for some $i2 \in \mathbb{Z}$ and then the assertion follows by taking $i = i2 * k$.

[1] Note that $m1$ is *not* arbitrary.

[2] Again, note that $m2$ is *not* arbitrary.

(E): $3 * j^2 + 3 * j - 24 = 3 * 2 * i - 6 * 4$, by **(D)** and arithmetic.

(F): $3 * j^2 + 3 * j - 24 = 6 * (i - 4)$, by **(E)** and arithmetic.

(G): We chose $m = i - 4$, and from **(F)** we obtain (α)

Note about the proof: Many of us would discover the need for **(A)** and **(C)** as we manipulate the formula for `f` $(k+1)$ and not separately, as the proof has been presented. We chose to separate the proof of **(B)** from the rest of the argument in order to improve readability.

(c) Take an arbitrary $j \in \mathbb{Z}$. The main idea of the proof is that `f` $(-j) = -($`f` $j)$ for our particular function `f`.

To show: $\exists i \in \mathbb{Z}.$ `f` $j = 6 * i$

1st Case: $j \geq 0$.

Then part (b) is applicable, and we obtain $\exists i \in \mathbb{Z}.$ `f` $j = 6 * i$.
Therefore we are done.

2nd Case: $j < 0$.

Then, $-j > 0$, and using part (b), we obtain that $\exists i' \in \mathbb{Z}.$ `f` $(-j) = 6 * i'$.
Then, using the fact that `f` $(-j) = -($`f` $j)$, we obtain that $-($`f` $j) = 6 * i'$.
Therefore, `f` $j = -(6 * i')$.
Therefore, `f` $j = 6 * (-i')$.
We now choose $i = -i'$, and obtain `f` $j = 6 * i$.
Therefore we obtain that $\exists i \in \mathbb{Z}.$ `f` $j = 6 * i$.

(d) We want to prove that
$\forall n \in \mathbb{Z}. \exists i \in \mathbb{Z}.$ `f` $n = 6 * i$.
The above assertion is equivalent with
$\forall n \in \mathbb{N}^+. \exists i \in \mathbb{Z}.$ `f` $n = 6 * i \quad \wedge$
$\exists i \in \mathbb{Z}.$ `f` $0 = 6 * i \quad \wedge$
$\forall n \in \mathbb{N}^+. \exists i \in \mathbb{Z}.$ `f` $(-n) = 6 * i$.
In part (b) we already prove the first two conjuncts. We can prove the last conjunct by mathematical induction.

(e) Let $P(n)$ be "all elements of `ff` k are divisible by 6". We will prove $\forall n \in \mathbb{N}. P(n)$ by mathematical induction.

Base case:

To show: all elements of the list `ff` 0 are divisible by 6.

By definition of `ff`, we know `ff` $0 = [0]$. Since 0 is divisible by 6, we are done.

Inductive Step:

Take an arbitrary $k \in \mathbb{N}$.
Inductive Hypothesis: all elements of `ff` k are divisible by 6
To show: all elements of `ff` $(k+1)$ are divisible by 6.

By definition of `ff`:
`ff` $(k+1) =$ `f` $(k+1)$: `ff` k
All elements of the list `ff` k are divisible by 6 by induction hypothesis. Furthermore,

`f` $(k+1)$ is divisible by 6, because of part (b). Therefore, all elements of the list `ff` $(k+1)$ are divisible by 6.

3rd Question:

Consider the program:

```
g :: Int -> Int
g 1 = 3
g 2 = 5
g n = (3*g (n-1)) - (2*g (n-2))
```

(a) For which values $n \in \mathbb{N}$ is `g` n defined?
For these values, give the value of `g` n in terms of n, but not in terms of another call of `g`.

(b) Prove your statement from part (a) by induction.

A possible answer:

(a) `g` is only defined for positive numbers.
Looking at some values of `g`, we obtain `g` $1 \ = 3$,
`g` $2 \ = 5$,
`g` $3 \ = 15 - 6 = 9$,
`g` $4 \ = 27 - 10 = 17$, and
`g` $5 \ = 51 - 18 = 33$.
Furthermore, we notice that
$2^1 + 1 = 3$,
$2^2 + 1 = 5$,
$2^3 + 1 = 9$,
$2^4 + 1 = 17$,
$2^5 + 1 = 33$.
We can generalize this into the following pattern

$$\forall n \in \mathbb{N}^+. \ \texttt{g} \ n = 2^n + 1$$

(b) Let $P(n)$ be `g` $n = 2^n + 1$. We will prove $\forall n \in \mathbb{N}^+. \ P(n)$ by strong induction.

Base case:

To show: `g` $1 = 2^1 + 1$.

`g` $1 = 3$, by definition of `g`, and $2^1 + 1 = 3$, by arithmetic.
Therefore we are done.

Inductive Step:

Take an arbitrary $k \in \mathbb{N}^+$.
Inductive Hypothesis $\forall m \in \{1..k\}. \ \texttt{g} \ m = 2^m + 1$
To show: `g` $(k+1) = 2^{k+1} + 1$

We need to distinguish the case where $k+1 = 2$ (and then `g` $2 = 5$) and the case where $k+1 > 2$ (and then `g` $(k+1) = (3 * \texttt{g} \ k) - (2 * \texttt{g} \ (k-1)))$.

1st Case: $k + 1 = 2$.

To show: $\mathtt{g}\ 2 = 2^2 + 1$.

$\mathtt{g}\ 2 = 5$, by definition of $\mathtt{g}$, and $2^2 + 1 = 5$, by arithmetic.
Therefore we are done.[3]

2nd Case: $k + 1 > 2$.

$$\begin{array}{lll}
\multicolumn{2}{l}{\mathtt{g}\ (k+1)} & \\
= & (3 * \mathtt{g}\ k) - (2 * \mathtt{g}\ (k-1)) & \text{because } k+1 > 2 \text{ and definition of } \mathtt{g} \\
= & (3 * (2^k + 1)) - (2 * (2^{k-1} + 1)) & \text{by ind. hyp. on } k \text{, and } k-1 \\
 & & \text{NOTE: ind. hyp. is applicable} \\
 & & \quad \text{because } 2 < k \leq k \\
 & & \quad \text{and } 1 < k-1 < k. \\
 & & \quad \text{and therefore } k, k-1 \in \{1..k\} \\
= & 3 * 2^k + 3 - 2 * 2^{k-1} - 2 & \text{by arithmetic} \\
= & 3 * 2^k - 2^k + 1 & \text{by arithmetic} \\
= & 2 * 2^k + 1 & \text{by arithmetic} \\
= & 2^{k+1} + 1 & \text{by arithmetic}
\end{array}$$

Therefore we are done.

4th Question

Consider the following function M which maps integers to integers, $M : \mathbb{Z} \longrightarrow \mathbb{Z}$, and which is defined as follows:

$$M(z) \;=\; \begin{cases} z - 10 & \text{if } z > 100; \\ M(M(z+11)) & z \leq 100. \end{cases}$$

We want to find a simple formula to describe the value of $M(z)$, for any $z \in \mathbb{Z}$.[4] To this end, we will discuss the following questions:

(a) What is the value of $M(104)$, $M(103)$, $M(102)$ and $M(101)$?

(b) What is the value of $M(100)$, $M(99)$, $M(98)$?

(c) Prove that for all z, where $90 < z < 101$, we have $M(z+1) = M(z)$. Prove also that for all z, where $90 < z < 101$, we have $M(z) = 91$.

(d) Calculate the value of $M(88)$, and $M(87)$.

(e) Calculate the value of $M(79)$, and $M(78)$.

(f) *This part is very challenging. More difficult than a standard exam question, but instructive.*

The value of $M(z)$ is described by an assertion of the form:
$\forall z \in \mathbb{Z}\, [\ z > 100 \to M(z) = z - 10 \ \wedge\ z \leq 100 \to M(z) =???\ ]$.

[3] Notice, that for this case we do not use the inductive hypothesis. However, we do make use of the inductive hypothesis in the next case.

[4] This is the famous McCarthy 91 function, further studied by by Zohar Manna, Amir Pnueli and Don Knuth, who all researched various fundamentals in computer science. I suggest you do not look up the function on wikipedia, and enjoy the exercise as given here.

Find an appropriate term for ???, and prove the assertion. Do not forget that z ranges over the integers, which include 0 as well as the negative numbers.

Hints: The proof of the assertion above consists of proving (A) and (B) from below:

$(A)\quad \forall z \in \mathbb{Z}\,[\ z > 100 \ \rightarrow\ M(z) = z - 10\ ]$
$(B)\quad \forall z \in \mathbb{Z}\,[\ z \leq 100 \ \rightarrow\ M(z) = ???\ ]$

We have already proven (A), and the challenge is to find ??? and then prove (B). Parts (a)-(e) should have given us some idea as to what the value of ??? can be. As to the proof of (B), remember the ideas in 2nd Question part c, on how to prove a property over $\mathbb{Z}$, rather than $\mathbb{N}$. Also, notice that the value of $M(100)$ is the base case, and that for $k < 100$ the value of $M(k)$ is a function of the value of $M(k+11)$, ie a *larger* value.

A possible answer:

(a) $M(104) = 94$, $M(103) = 93$, $M(102) = 92$ and $M(101) = 91$, according to the first case in the definition of M.

(b) We now calculate the values of $M(100)$, $M(99)$, $M(98)$:

$$\begin{array}{lcll} M(100) & = & M(M(111)) & \text{because } 100 \leq 100\text{, and definition of } M \\ & = & M(101) & \text{because } 111 > 100\text{, and definition of } M \\ & = & 91 & \text{because, as shown in 1., we have that } M(101) = 91. \end{array}$$

The other terms follow the same pattern, *i.e.*

$M(99) = M(M(110)) = M(100) = 91$
$M(98) = M(M(109)) = M(99) = 91$

(c) We now prove that $\forall z \in \mathbb{Z} :\ (90 \leq z \leq 100) \Longrightarrow M(z+1) = M(z)$.

Proof. We take an arbitrary $z \in \mathbb{Z}$, with $(90 \leq z \leq 100)$.

$$\begin{array}{lcll} M(z) & = & M(M(z+11)) & \text{because } z \leq 100\text{, and definition of } M \\ & = & M(z+11-10) & \text{because } z+11 \geq 90+11 > 100\text{, and definition of } M \\ & = & M(z+1) & \text{by arithmetic.} \end{array}$$

The results from (b) and (c) also give us that
$(*)\quad \forall z \in \mathbb{Z}.\,[\ 90 \leq z \leq 100\ \rightarrow\ M(z) = 91\ ]$

(d) Now calculate $M(88)$, and $M(87)$.

$$\begin{array}{lcll} M(88) & = & M(M(99)) & \text{because } 88 \leq 100\text{, and definition of } M \\ & = & M(91) & \text{because } 99 \leq 100\text{, and definition of } M \\ & = & 91 & \text{by } (*). \end{array}$$

By similar argument, we obtain that $M(87) = 91$.

(e) We will not *calculate* the values of $M(79)$ and $M(78)$. Instead, we will move to part (f) directly.

(f) We will prove that
$(**)\quad \forall z \in \mathbb{Z}.\ [\ z \leq 100\ \rightarrow\ M(z) = 91\ ]$

The assertion (**) follows from (*) from above, and the following assertion (***):

$(***)\quad \forall n \in \mathbb{N}.\, M(100 - n) = 91.$

Note that we now have an assertion of $n \in \mathbb{N}$; therefore we can now can prove (***) by strong induction over n. [5]

Base case:

To show: $M(100) = 91$.

This follows from part (b).

Inductive Step:

Take an arbitrary $k \in \mathbb{N}$.
Inductive Hypothesis: $\forall i \in [0..k].\, M(100 - i) = 91$.
To show: $M(100 - (k + 1)) = 91$

First Case: $k \leq 9$.

Since, $k \leq 9$, we have that $90 < 100 - (k + 1) < 100$, and the assertion follows from $(*)$ in part c.

Second Case: $k \geq 10$.

$$
\begin{array}{lll}
\text{M(100-(k+1))} & = \text{M(M(100-(k+1)+11))} & \text{because } k+1 \text{ is positive,} \\
 & & \text{thus } 100-(k+1) \leq 100; \\
 & & \text{apply definition of } M \\
 & = \text{M(M(100-(k-10)))} & \text{by arithmetic} \\
 & = \text{M(91)} & \text{by induction hypothesis,} \\
 & & \text{which is applicable,} \\
 & & \text{because } k-10 \in [0..k] \\
 & = 91 & \text{part c.}
\end{array}
$$

Note: the case analysis was necessary in order to ascertain that in the second case $k - 10 \in [0..k]$, and thus be able to apply the inductive hypothesis.

Acknowledgements:

Some of the questions on this PMT sheet are based on earlier material by Jeremy Bradley, Francesca Toni, Robert Craven, Krysia Broda, Ian Hodkinson, Xiang Feng.

[5] The wikipedia article on the McCarthy function shows a slightly different proof, which uses mathematical induction, and argues in terms of overlapping intervals. I think that the proof given here is more elegant; what do you think?