DMMR Tutorial sheet 4

Induction

October 10th, 2019

1. Use strong induction to show that every positive integer n can be written as a sum of distinct powers of two, that is, as a sum of a subset of the integers $2^0 = 1$, $2^1 = 2$, $2^2 = 4$, and so on.

   Before beginning your proof, state the property (the one you are asked to prove for every integer n) in completely formal notation with all quantifiers.

   Solution:
   The sentence we are required to prove can be stated formally as follows:

$$\forall\, n \in \mathbb{Z}^+ \;\exists\, m \in \mathbb{Z}^+ \;\exists\, a_1, a_2, a_3, \ldots, a_m \in \mathbb{N}$$
$$[(\forall\, i, j \in \{1, \ldots, m\}\; i \neq j \longrightarrow a_i \neq a_j) \wedge n = 2^{a_1} + 2^{a_2} + \cdots + 2^{a_m}]$$

   or more concisely as follows:

$$\forall\, n \in \mathbb{Z}^+ \;\exists\, S \subseteq \mathbb{N} \left(n = \sum_{a \in S} 2^a \right)$$

   Base case: The sum with a single element 2^0 equals 1.

   Induction hypothesis: We assume that every l, with $l \leq k$, is the sum of distinct powers of two and then prove it for $k+1$ by splitting into the two cases $k+1$ is even and $k+1$ is odd.

   Induction step: *Case 1:* If $k+1$ is even then $(k+1)/2$ is an integer and $(k+1)/2 \leq k$. Using the induction hypothesis we can write $(k+1)/2$ as $2^{a_1} + 2^{a_2} + \cdots + 2^{a_m}$ where all a_i's are distinct. Then,

$$\begin{aligned} k+1 &= 2(2^{a_1} + 2^{a_2} + \cdots + 2^{a_m}) \\ &= 2 \cdot 2^{a_1} + 2 \cdot 2^{a_2} + \cdots + 2 \cdot 2^{a_m} \\ &= 2^{a_1+1} + 2^{a_2+1} + \cdots + 2^{a_m+1} \end{aligned}$$

   These are clearly distinct powers of two, thus we have proved what we wanted.

   Case 2: If $k+1$ is odd we apply the induction hypothesis to k to get $k = 2^{a_1} + 2^{a_2} + \cdots + 2^{a_m}$. However, we know that $a_i \neq 0$ for every i with $1 \leq i \leq m$ because otherwise exactly one element of the sum would be $2^0 = 1$ and the rest would be even, and thus k would be odd. Therefore,

$$\begin{aligned} k+1 &= 2^{a_1} + 2^{a_2} + \cdots + 2^{a_m} + 1 \\ &= 2^{a_1} + 2^{a_2} + \cdots + 2^{a_m} + 2^0 \end{aligned}$$

   and $\{2^{a_1}, 2^{a_2}, \cdots, 2^{a_m}, 2^0\}$ are all distinct. $\square$

2. What is wrong with this "proof"?

   "Theorem" For every positive integer n, if x and y are positive integers with $\max(x, y) = n$, then $x = y$.

   Base case: Suppose that $n = 1$. If $\max(x, y) = 1$ and x and y are positive integers, we have $x = 1$ and $y = 1$.

   Induction hypothesis: Let k be a positive integer. Assume that whenever $\max(x, y) = k$ and x and y are positive integers, then $x = y$. Now let $\max(x, y) = k + 1$, where x and y are positive integers.

   Induction step: Then $\max(x - 1, y - 1) = k$, so by the induction hypothesis, $x - 1 = y - 1$. It therefore follows that $x = y$, completing the induction step.

   Solution:
   The result is clearly false, so the proof must be wrong. The base case proof is correct, so the problem has to be in the induction step. The induction hypothesis is stated correctly and it is true that if $\max(x, y) = k + 1$ then $\max(x - 1, y - 1) = k$, so the problem must be in *applying* the induction hypothesis. Analysing the induction hypothesis we see that it requires the numbers to be positive integers to conclude that they are equal. However, it is applied to the predecessors $x - 1$ and $y - 1$ of two positive integers, which are not necessarily positive. By incrementing the size of k starting from its value in the base case (1) we can find the place where the chain of dominoes (as described in the textbook) first *breaks*. For $k = 2$ take $x = 2$ and $y = 1$. Then, $max(x, y) = 2$. However, $x - 1 = 1$ and $y - 1 = 0$. These numbers are not the values of x and y that we used in the base case; and if 0 had been allowed we would not have been able to prove the base case. Thus, the induction chain breaks after the first domino. $\square$

3. Let $n \geq 0$ be an integer. Prove by induction:

   (a) 8 divides $3^{2n+2} + 7$

   (b) 64 divides $3^{2n+2} + 56n + 55$

   Solution:

   (a) We prove this by induction over n:
   Base case: For $n = 0$ we get $3^2 + 7 = 9 + 7 = 16$. 8 divides 16 since $16 = 2 \cdot 8$
   Induction hypothesis: Assume 8 divides $3^{2n+2} + 7$.
   Induction step: with (n+1) we get

$$
\begin{aligned}
&3^{2(n+1)+2} + 7 \\
=&3^{2n+2+2} + 7 \\
=&3^{2n+2} \cdot 9 + 7 \\
=&3^{2n+2} \cdot 8 + 3^{2n+2} + 7
\end{aligned}
$$

   By the IH we know that $3^{2n+2} + 7$ is presentable as $c \cdot 8$. Therefore we get $3^{2(n+1)+2} + 7 = (3^{2n+2} + c) \cdot 8$. Since $(3^{2n+2} + c) \in \mathbb{Z}$ this means 8 divides $3^{2(n+1)+2} + 7$ by definition.
   By the induction principle 8 divides $(3^{2n+2} + 7)$ for every $n \geq 0$

   (b) Proof by induction over n:
   Base case: For $n = 0$ we get $3^2 + 55 = 9 + 55 = 64$. 64 divides 64 since $64 \cdot 1 = 64$.
   Induction hypothesis: Assume 64 divides $3^{2n+2} + 56n + 55$ for some $n \geq 0$

Induction step: For $n+1$ we get:

$$\begin{aligned}
&3^{2(n+1)+2} + 56(n+1) + 55 \\
=&3^{2n+2} + 56n + 55 + 3^{2n+2} \cdot 8 + 56 \\
=&3^{2n+2} + 56n + 55 + (3^{2n+2} + 7) \cdot 8
\end{aligned}$$

From the IH we know 64 divides $3^{2n+2}+56n+55$ and therefore $3^{2n+2}+56n+55 = 64 \cdot c$ for some $c \in \mathbb{Z}$. From a) we know that 8 divides $(3^{2n+2}+7)$ and therefore $(3^{2n+2}+7) = 8 \cdot c'$ for some $c' \in \mathbb{Z}$. This means $(3^{2n+2}+7) \cdot 8 = c' \cdot 8 \cdot 8 = c' \cdot 64$. Together we get $3^{2(n+1)+2} + 56(n+1) + 55 = 64 \cdot (c + c')$. Since $c + c' \in \mathbb{Z}$ this means 64 divides $3^{2(n+1)+2} + 56(n+1) + 55$ by definition.

By the induction principle 64 divides $(3^{2n+2} + 56n + 55)$ for every $n \geq 0$

$\square$

4. A finite continued fraction is either an integer n or of the form $n + (1/F)$ where F is a finite continued fraction. For example, $7/9 = 0 + 1/(9/7)$, $9/7 = 1 + 1/(7/2)$, $7/2 = 3 + 1/2$; so, $7/9 = 0 + 1/(1 + 1/(3 + 1/2))$. Similarly, $17/14 = 1 + 1/(4 + 1/(1 + 1/2))$. What you have to prove is that every rational can be expressed as a finite continued fraction. Let $P(k)$ be "any rational with denominator k can be expressed as a finite continued fraction". Prove by strong induction $\forall x \in \mathbb{Z}^+(P(x))$.

   In your proof you can use the division algorithm: if a is an integer and d a positive integer then there are unique integers q and r, with $0 \leq r < d$ such that $a = dq + r$.

   Solution:
   Base case: Show $P(1)$. Consider any rational with denominator 1. Assume it is $n/1$. Since n is a continued fraction and $n = n/1$, $P(1)$ holds.

   Induction step: Assume that for some $d \in \mathbb{Z}^+$ with $d > 1$ that for any $k \in \mathbb{Z}^+$, $1 \leq k < d$, $P(k)$ is true; so, any rational with denominator k can be expressed as a continued fraction. We show $P(d)$. Consider a rational n/d with denominator d. Use the division algorithm and write $n = dq + r$ where $0 \leq r < d$. We split into two cases.

   (a) $r = 0$. Then $n = dq$ so $n/d = q$ and, therefore, q is a continued fraction for n/d.

   (b) $r \neq 0$. Since $n = dq + r$, it follows that $n/d = q + r/d = q + 1/(d/r)$. As $1 \leq r < d$ by the inductive hypothesis there is a continued fraction F for d/r. Therefore, $q + 1/F$ is a continued fraction for n/d.

$\square$

5. Two sequences $\{a_n\}_{n \in \mathbb{Z}^+}$ and $\{b_n\}_{n \in \mathbb{Z}^+}$ are defined recursively as follows.

$$\begin{array}{lll}
a_1 = 1 & \text{for } n \geq 1 & a_{n+1} = a_n + 2b_n \\
b_1 = 1 & \text{for } n \geq 1 & b_{n+1} = a_n + b_n
\end{array}$$

   Prove by induction that for all $n \in \mathbb{Z}^+$, $a_n^2 - 2b_n^2 = (-1)^n$.

   Solution:
   Base Case: $n = 1$ and $a_1^2 - 2b_1^2 = -1$.

Induction step Assume true for k, that $a_k^2 - 2b_k^2 = (-1)^k$, we now show it holds for $k+1$.

$$\begin{array}{rcl}
a_{k+1}^2 - 2b_{k+1}^2 & = & (a_k + 2b_k)^2 - 2(a_k + b_k)^2 \text{ by definition of the sequences} \\
& = & a_k^2 + 4b_k^2 + 4a_kb_k - 2(a_k^2 + b_k^2 + 2a_kb_k) \\
& = & -1(a_k^2 - 2b_k^2) \\
& = & -1(-1)^k \quad \text{by induction hypothesis} \\
& = & (-1)^{k+1}
\end{array}$$

□