Housekeeping

Assignment solutions 1 are now available.

Assignment 3 is available and is due at the beginning of your support class in week 5 (27 – 31 Mar).

Tutorial sheet 3 and tutorial solutions 2 are also available.

MAT1830

Lecture 10: Induction and well-ordering

n	0	1	2	3	4	5	6	7	8	$\cdots$
$P(n)$	T	T	T	T	T	T	T	T	T	$\cdots$

Let $a_0, a_1, a_2, a_3, \ldots$ be a sequence defined by

$$a_0 = 2, \quad a_1 = 6, \quad a_n = a_{n-1} + a_{n-2} \text{ for all } n \geq 2.$$

So it goes $2, 6, 8, 14, 22, 36, 58, \ldots$.

Question Prove that a_n is even for all $n \geq 0$.

Proof Let $P(n)$ be the statement "a_n is even".

Base Steps. Note that $a_0 = 2$ and $a_1 = 6$ are even, so $P(0)$ and $P(1)$ are true.

Induction Step. Suppose that $P(0), P(1), \ldots, P(k)$ are true for some integer $k \geq 1$. This means that $a_0, a_1, \ldots, a_k$ are all even.

We want to prove that $P(k+1)$ is true. We need to show that a_{k+1} is even.

$$a_{k+1} = a_k + a_{k-1}$$

a_k is even because $P(k)$ is true and a_{k-1} is even because $P(k-1)$ is true.
So a_{k+1} is even.

Thus $P(n)$ is true for all $n \geq 0$.

In the previous lecture we were able to prove a property P holds for $0, 1, 2, \ldots$ as follows:

Base step. Prove $P(0)$

Induction step. Prove $P(k) \Rightarrow P(k+1)$ for each natural number k.

This is sufficient to prove that $P(n)$ holds for all natural numbers n, but it may be difficult to prove that $P(k+1)$ follows from $P(k)$. It may in fact be easier to prove the induction step

$$\boxed{P(0) \wedge P(1) \wedge \cdots \wedge P(k) \Rightarrow P(k+1).}$$

That is, it may help to assume P holds for *all* numbers before $k+1$. Induction with this style of induction step is sometimes called the *strong form* of mathematical induction.

Example 1. Prove that, for each integer $n \geq 2$, n has a prime factorisation.

Solution Let $P(n)$ be the statement "n has a prime factorisation".

Base step. 2 is prime. So just '2' is a prime factorisation for 2.

Induction step. Suppose that $P(2), P(3), \ldots, P(k)$ are true for some integer $k \geq 2$. This means that $2, 3, \ldots, k$ all have prime factorisations.

We want to prove that $P(k+1)$ is true. We need to show that $k+1$ has a prime factorisation.

If $k+1$ is prime, then just '$k+1$' is a prime factorisation for $k+1$.

If $k+1$ is not prime, then $k+1 = i \times j$ for integers i, j such that $2 \leq i, j \leq k$.
Because $P(i)$ is true i has a prime factorisation.
Because $P(j)$ is true j has a prime factorisation.
So $i \times j$ has a prime factorisation. (Just combine the prime factorisations of i and j.)

So $P(k+1)$ is true.

This proves that $P(n)$ is true for each integer $n \geq 2$.

Question 10.1 Which of the following is likely to require strong induction for its proof.

$$1 + a + a^2 + \cdots + a^n = \frac{a^{n+1} - 1}{a - 1}$$

No - normal induction is enough. This is very similar to Q4 from Assignment 3.

$$\neg(p_1 \vee p_2 \vee \cdots \vee p_n) \equiv \neg p_1 \wedge \neg p_2 \wedge \cdots \wedge \neg p_n$$

No - normal induction is enough. $\neg(p_1) \equiv \neg p_1$ and if we assume the statement is true for $n = k$ then

$$\begin{aligned} \neg(p_1 \vee p_2 \vee \cdots \vee p_k \vee p_{k+1}) &\equiv \neg((p_1 \vee p_2 \vee \cdots \vee p_k) \vee p_{k+1}) \\ &\equiv \neg(p_1 \vee p_2 \vee \cdots \vee p_k) \wedge \neg p_{k+1} \\ &\equiv (\neg p_1 \wedge \neg p_2 \wedge \cdots \wedge \neg p_k) \wedge \neg p_{k+1} \\ &\equiv \neg p_1 \wedge \neg p_2 \wedge \cdots \wedge \neg p_k \wedge \neg p_{k+1} \end{aligned}$$

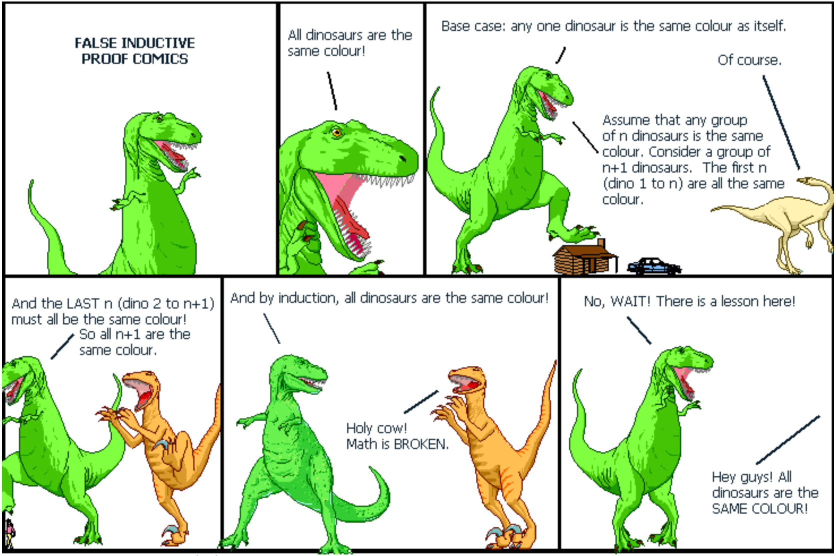
as required.

Prove that the every integer in the sequence $a_0, a_1, a_2, a_3, \ldots$ defined by

$$a_0 = 2, \quad a_1 = 6, \quad a_n = a_{n-1} + a_{n-2} \text{ for all } n \geq 2$$

is even.

Yes. We just saw it does.



(C) 2004 ~~Ryan North~~ Jon Sharkey
www.qwantz.com

Examples for “Example 2”

$14 = 8 + 4 + 2 = 2^3 + 2^2 + 2^1$.

$34 = 32 + 2 = 2^5 + 2^1$.

NOT $14 = 4 + 4 + 4 + 1 + 1$. (Not *distinct*.)

Example 2. Every integer $\geqslant 1$ is a sum of distinct powers of 2.

The idea behind this proof is to repeatedly subtract the largest possible power of 2. We illustrate with the number 27.

$$\begin{aligned} 27 &- \text{largest power of 2 less than } 27 \\ &= 27 - 16 = 11 \\ 11 &- \text{largest power of 2 less than } 11 \\ &= 11 - 8 = 3 \\ 3 &- \text{largest power of 2 less than } 3 \\ &= 3 - 2 = 1 \end{aligned}$$

Hence $27 = 16 + 8 + 2 + 1 = 2^4 + 2^3 + 2^1 + 2^0$.

(It is only interesting to find *distinct* powers of 2, because of course each integer $\geqslant 1$ is a sum of 1s, and $1 = 2^0$.)

More examples for “Example 2”

$\mathbf{k+1=14}$:

Assume that $1, \ldots, 13$ can be written as a sum of distinct powers of 2.
Subtract the largest power of 2 which is at most 14: $14 - 2^3 = 6$
By assumption, 6 can be written as a sum of distinct powers of 2: $6 = 2^2 + 2^1$
So $14 = 2^3 + 6 = 2^3 + 2^2 + 2^1$.

$\mathbf{k+1=81}$:

Assume that $1, \ldots, 80$ can be written as a sum of distinct powers of 2.
Subtract the largest power of 2 which is at most 81: $81 - 2^6 = 17$
By assumption, 17 can be written as a sum of distinct powers of 2: $17 = 2^4 + 2^0$
So $81 = 2^6 + 17 = 2^6 + 2^4 + 2^0$.

$\mathbf{k+1=128}$:

Assume that $1, \ldots, 127$ can be written as a sum of distinct powers of 2.
Subtract the largest power of 2 which is at most 128: $128 - 2^7 = 0$
So $128 = 2^7$.

Example 2. Prove that, for each integer $n \geq 1$, n can be written as a sum of distinct powers of 2.

Solution Let $P(n)$ be the statement "n can be written as a sum of distinct powers of 2".

Base step. $1 = 2^0$, so 1 is a sum of (one) power of 2.

Induction step. Suppose that $P(1), P(2), \ldots, P(k)$ are true for some integer $k \geq 1$. This means that $1, 2, \ldots, k$ can each be written as a sum of distinct powers of 2.

We want to prove that $P(k+1)$ is true. We need to show that $k+1$ can be written as a sum of distinct powers of 2.

If $k+1$ is a power of 2, then we are finished.

If not, let 2^j be the greatest power of 2 less than $k+1$.
(This means that $2^j > \frac{1}{2}(k+1)$.)
Let $i = (k+1) - 2^j$. Note that $1 \leq i < 2^j$.
Because $P(i)$ is true, i can be written as a sum of distinct powers of 2.
(Note that each power of 2 in this sum is smaller than 2^j because $i < 2^j$.)
So $k+1 = 2^j + i$ can be written as a sum of distinct powers of 2.

So $P(k+1)$ is true.

This proves that $P(n)$ is true for each integer $n \geq 2$.

Question 10.2 What else tells you every integer is a sum of distinct powers of 2?

The fact that every integer can be written in binary is equivalent to saying every integer is a sum of distinct powers of 2.

Question 10.3 Is every integer ≥ 1 a sum of distinct powers of 3?

No. The powers of three are $1, 3, 9, 27, \ldots$. So, for example, 2 is not and 7 is not.

We can write every integer ≥ 1 as

$$a_0 3^0 + a_1 3^1 + a_2 3^2 + a_3 3^3 + \cdots$$

where $a_0, a_1, a_2, a_3, \ldots$ are all in $\{0, 1, 2\}$, however.

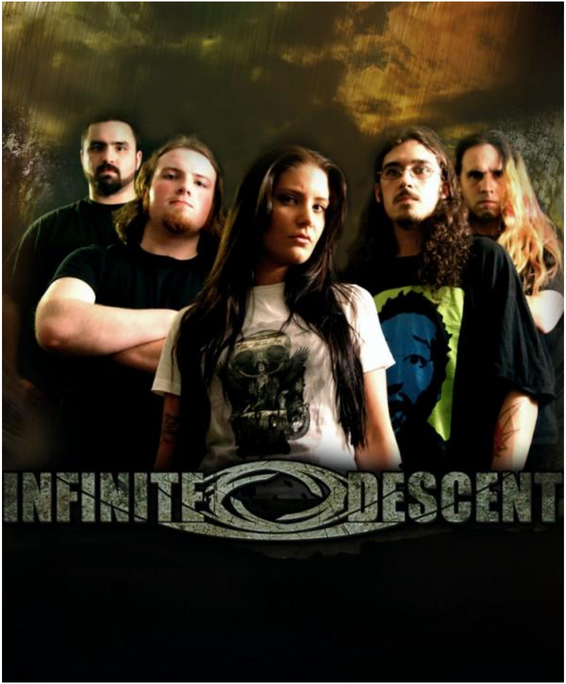
10.2 Well-ordering and descent

Induction expresses the fact that each natural number n can be reached by starting at 0 and going upwards (e.g. adding 1) a finite number of times.

Equivalent facts are that it is only a finite number of steps *downwards* from any natural number to 0, that *any descending sequence of natural numbers is finite*, and that *any set of natural numbers has a least member*.

This property is called *well-ordering* of the natural numbers. It is often convenient to arrange a proof to "work downwards" and appeal to well-ordering by saying that the process of working downwards must eventually stop.

Such proofs are equivalent to induction, though they may be called "infinite descent" or some such name.


INFINITE DESCENT

10.3 Proofs by descent

Example 1. Existence of a prime divisor

If n is any natural number $\geqslant 2$, then n has a prime divisor.

Proof. If n is prime, then it is a prime divisor of itself. If not, let $n_1 < n$ be a divisor of n.

If n_1 is prime, it is a prime divisor of n. If not, let $n_2 < n_1$ be a divisor of n_1 (and hence of n).

If n_2 is prime, it is a prime divisor of n. If not, let $n_3 < n_2$ be a divisor of n_2, etc.

The sequence $n > n_1 > n_2 > n_3 > \cdots$ must eventually terminate, and this means we find a prime divisor of n.

Question Is every descending sequence of positive rational numbers finite?

No. For example $\frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \ldots$ is an infinite sequence.

Example 2. Irrationality of $\sqrt{2}$

Suppose that $\sqrt{2} = m/n$ for natural numbers m and n. Since the square of an odd number is odd, we can argue as follows

$$\begin{aligned}
& \sqrt{2} = m/n \\
\Rightarrow\quad & 2 = m^2/n^2 \\
& \text{squaring both sides} \\
\Rightarrow\quad & m^2 = 2n^2 \\
\Rightarrow\quad & m^2 \text{ is even} \\
\Rightarrow\quad & m \text{ is even} \\
& \text{since the square of an odd number is odd} \\
\Rightarrow\quad & m = 2m_1 \text{ say} \\
\Rightarrow\quad & 2n^2 = m^2 = 4m_1^2 \\
\Rightarrow\quad & n^2 = 2m_1^2 \\
\Rightarrow\quad & n \text{ is even, } = 2n_1 \text{ say}
\end{aligned}$$

But then $\sqrt{2} = m_1/n_1$, and we can repeat the argument to show that m_1 and n_1 are both even, so $m_1 = 2m_2$ and $n_1 = 2n_2$, and so on.

Since the argument can be repeated indefinitely, we get an *infinite* descending sequence of natural numbers

$$m > m_1 > m_2 > \cdots$$

which is impossible.

Hence there are no natural numbers m and n with $\sqrt{2} = m/n$.