CSC B36 Additional Notes

sample induction and well-ordering proofs

© Nick Cheng

⋆ Introduction

We present examples of induction proofs here in hope that they can be used as models when you write your own proofs. These include simple, complete and structural induction. We also present a proof using the Principle of Well-Ordering, and two pretend[1] induction proofs.

⋆ A Simple Induction Proof

Problem:

Prove that for all natural numbers $n > 4$, $2^n > n^2$.

Solution:

Base Case: Let $n = 5$.
Then $2^n = 2^5 = 32$ and $n^2 = 5^2 = 25$.
So $2^n > n^2$ as wanted.

Induction Step: Let $n \geq 5$.
Suppose $2^n > n^2$. [IH]
WTP: $2^{n+1} > (n+1)^2$.

$$\begin{aligned} 2^{n+1} &= 2 \cdot 2^n \\ &= 2^n + 2^n \\ &> n^2 + n^2 && \text{[IH (twice)]} \\ &\geq n^2 + 5n && \text{[since } n \geq 5,\ n^2 = n \cdot n \geq 5n\text{]} \\ &> n^2 + 2n + 1 && \text{[since } 5n = 2n + 3n > 2n + 1\text{]} \\ &= (n+1)^2 \end{aligned}$$

as wanted. □

[1] *Pretend induction* is a term invented by yours truly, and used only in this course when I teach it. Searching for any literature on it is not recommended.

⋆ A Complete Induction Proof

Problem:

Consider the function $f : \mathbb{N} \to \mathbb{N}$ defined recursively as follows.

$$f(n) = \begin{cases} n & \text{if } 0 \leq n \leq 2; \\ 3f(n-2) + 2f(n-3) & \text{if } n > 2. \end{cases}$$

Prove that $f(n) < 2^n$ for all $n \in \mathbb{N}$.

Solution:

Base Cases: Consider cases where $0 \leq n \leq 2$.

If $n = 0$,

then $f(n) = 0$ [definition of f]

$< 1 = 2^0 = 2^n$ as wanted.

If $n = 1$,

then $f(n) = 1$ [definition of f]

$< 2 = 2^1 = 2^n$ as wanted.

If $n = 2$,

then $f(n) = 2$ [definition of f]

$< 4 = 2^2 = 2^n$ as wanted.

Induction Step:

Let $n > 2$.

Suppose $f(j) < 2^j$ whenever $0 \leq j < n$. [IH]

WTP: $f(n) < 2^n$.

$f(n) = 3f(n-2) + 2f(n-3)$ [definition of f; $n > 2$]

$< 3 \cdot 2^{n-2} + 2 \cdot 2^{n-3}$ [IH; $0 \leq n-3 < n-2 < n$]

$= 6 \cdot 2^{n-3} + 2 \cdot 2^{n-3}$ [express using common term 2^{n-3}]

$= 8 \cdot 2^{n-3}$

$= 2^n$

as wanted. □

⋆ A Structural Induction Proof

Definition for problem:

Given $n, m \in \mathbb{Z}$, we say that n *divides* m, denoted $n|m$, iff there is some $k \in \mathbb{Z}$ such that $m = kn$.

Problem:

Let $a, b, c \in \mathbb{Z}$ with $c|a$ and $c|b$. We use structural induction to define G, which is a set of ordered pairs of integers. I.e., $G \subseteq \mathbb{Z}^2$.

> Let G be the smallest set such that
> Basis: $(a, b) \in G$.
> Induction Step: If $(u, v) \in G$, then $(u, v - u) \in G$ and $(u - v, v) \in G$.

Prove that for any $(x, y) \in G$, $c|x$ and $c|y$.

Loosely speaking, if we start with a pair of integers (a, b) that are divisible by c, then any other pair that can be generated by using the induction step above as many times as we want are also divisible by c. This result is useful in proving correctness of Euclid's algorithm for finding the gcd (greatest common divisor) of two numbers. Do you see how?

Solution:

Base Case: Let $(x, y) = (a, b)$.
Then $c|x$ and $c|y$ [since we are given $c|a$ and $c|b$] as wanted.

Induction Step: Let $(x, y) \in G$.
Suppose $c|x$ and $c|y$ (i.e., there are $i, j \in \mathbb{Z}$ such that $x = ic$ and $y = jc$). [IH]
WTP: For any (x', y') that can be constructed from (x, y) using one induction step, $c|x'$ and $c|y'$.

We have two cases: $(x', y') = (x, y - x)$ and $(x', y') = (x - y, y)$.

For $(x', y') = (x, y - x)$, let $i' = i$ and $j' = j - i$.
Since $i, j \in \mathbb{Z}$, we have $i', j' \in \mathbb{Z}$.
Also, $x' = x$
$= ic$ [IH]
$= i'c$

and $y' = y - x$
$= jc - ic$ [IH]
$= (j - i)c$
$= j'c$.
Thus $c|x'$ and $c|y'$ as wanted.

For $(x', y') = (x - y, y)$, let $i' = i - j$ and $j' = j$.
Since $i, j \in \mathbb{Z}$, we have $i', j' \in \mathbb{Z}$.
Also, $x' = x - y$
$= ic - jc$ [IH]
$= (i - j)c$
$= i'c$

and $y' = y$
$= jc$ [IH]
$= j'c$.
Thus $c|x'$ and $c|y'$ as wanted. □

⋆ A Principle of Well-Ordering (PWO) Proof

Definitions for problem:

A sequence of numbers $b_0, b_1, b_2, \cdots$ is said to be *bounded above* iff there is some $B \in \mathbb{N}$ such that $b_i \leq B$ for any i where b_i is defined. In this case, B is said to be an *upper bound* of the sequence.

A sequence of numbers $b_0, b_1, b_2, \cdots$ is said to be *increasing* iff $b_i < b_{i+1}$ for any i where both b_i and b_{i+1} are defined.

Problem:

Prove that every bounded (above) increasing sequence of natural numbers is finite.

Solution:

Let $b_0, b_1, b_2, \cdots$ be a bounded (above) increasing sequence of natural numbers.
Let U be an upper bound of our sequence. So $U \in \mathbb{N}$.

By way of contradiction, suppose the sequence $b_0, b_1, b_2, \cdots$ is infinite.

Consider the set A defined by
$A = \{n : n = U - b_i \text{ for some } i \in \mathbb{N}\}$ (i.e., A is the set of all numbers of form $U - b_i$).

$A \subseteq \mathbb{N}$ because each $b_i \leq U$.
Also, A is nonempty because $U - b_0 \in A$.
Thus by PWO, A has a minimum element.

Let m be a minimum element of A.
Then $m = U - b_j$ for some $j \in \mathbb{N}$.

Now consider $m' = U - b_{j+1}$.
By definition of A, we have $m' \in A$.
Also, $m' = U - b_{j+1}$
$< U - b_j$ [since sequence is increasing, $b_{j+1} > b_j$]
$= m$.
Thus $m' < m$, which contradicts m being a minimum element of A.

Therefore the sequence $b_0, b_1, b_2, \cdots$ is finite. □

⋆ A Pretend (complete) Induction Proof

Problem:

Consider the following inductively defined function.

$$f(n) = \begin{cases} n & \text{if } 1 \le n \le 2; \\ 2f(\lfloor \frac{n}{2} \rfloor) + \lfloor \sqrt{n} \rfloor & \text{if } n > 2. \end{cases}$$

Find positive constants c and d so that $f(n) \le cn - d\sqrt{n}$ for all integers $n \ge 1$.

Solution:

We use pretend induction.

Base Cases: Consider cases $n = 1$ and $n = 2$.

If $n = 1$,
then $f(n) = 1$ [definition of f]
and $cn - d\sqrt{n} = c - d$.
So we need $1 \le c - d$. **(*)**

If $n = 2$,
then $f(n) = 2$ [definition of f]
and $cn - d\sqrt{n} = 2c - \sqrt{2}d$.
So we need $2 \le 2c - \sqrt{2}d$. **(**)**

Since (*) implies (**), we just need $1 \le c - d$, or equivalently,

$$c \ge d + 1. \quad \textbf{(\#)}$$

Induction Step: Let $n > 2$.

Suppose $f(j) \le cj - d\sqrt{j}$ whenever $1 \le j < n$. [IH]
WTP: $f(n) \le cn - d\sqrt{n}$.

$$\begin{aligned} f(n) &= 2f(\lfloor \tfrac{n}{2} \rfloor) + \lfloor \sqrt{n} \rfloor && \text{[definition of } f\text{; } n > 2\text{]} \\ &\le 2\left(c\lfloor \tfrac{n}{2} \rfloor - d\sqrt{\lfloor \tfrac{n}{2} \rfloor}\right) + \lfloor \sqrt{n} \rfloor && \text{[IH; } 1 \le \lfloor \tfrac{n}{2} \rfloor < n \text{ if } n > 2\text{]} \\ &\le 2c\tfrac{n}{2} - 2d\sqrt{\tfrac{n-1}{2}} + \sqrt{n} && \text{[} \tfrac{n-1}{2} \le \lfloor \tfrac{n}{2} \rfloor \le \tfrac{n}{2}\text{; } \lfloor \sqrt{n} \rfloor \le \sqrt{n} \text{]} \\ &= cn - \sqrt{2(n-1)}d + \sqrt{n} && \text{[simplify]} \end{aligned}$$

So to get $f(n) \le cn - d\sqrt{n}$, we need

$$cn - \sqrt{2(n-1)}d + \sqrt{n} \le cn - d\sqrt{n}. \quad \textbf{(***)}$$

Subtracting cn from both sides and isolating d, (***) becomes

$$d \ge \frac{\sqrt{n}}{\sqrt{2(n-1)} - \sqrt{n}},$$

and this must be true for all $n > 2$ (so the induction would work).

Therefore we need $d \ge \max\limits_{n>2} \left\{ \frac{\sqrt{n}}{\sqrt{2(n-1)} - \sqrt{n}} \right\}$

$$\begin{aligned} &= \tfrac{\sqrt{3}}{2-\sqrt{3}} && \text{[maximum occurs at } n = 3\text{]} \\ &\approx 6.464\cdots \quad \textbf{(\#\#)} \end{aligned}$$

Finally, we choose c and d so that (#) and (##) are satisfied.
For example, we can pick $d = 7$ and $c = 8$. □

⋆ A Pretend (simple) Induction Proof

This example is less complex than the previous one.

Problem:

Consider the following inductively defined function.

$$f(n) = \begin{cases} 7 & \text{if } n = 0; \\ 2f(n-1) + 3 & \text{if } n > 0. \end{cases}$$

Find positive constants c and d so that $f(n) \leq c\,2^n - d$ for all $n \in \mathbb{N}$.

Solution:

We use pretend induction.

Basis: Let $n = 0$.

Then $f(n) = 7$ [definition of f] and $c\,2^n - d = c - d$.
We want $f(n) \leq c\,2^n - d$.
So we need $7 \leq c - d$, or equivalently, $c \geq d + 7$. **(*)**

Induction Step: Let $n \geq 0$.

Suppose $f(n) \leq c\,2^n - d$. [IH]
WTP: $f(n+1) \leq c2^{n+1} - d$.

$$\begin{aligned} f(n+1) &= 2f(n) + 3 && \text{[definition of } f\text{; } n+1 > 0\text{]} \\ &\leq 2(c\,2^n - d) + 3 && \text{[IH]} \\ &= c\,2^{n+1} - 2d + 3. && \text{[isolate } c\,2^{n+1} \text{ term]} \end{aligned}$$

We want $f(n+1) \leq c\,2^{n+1} - d$.
So we need $c\,2^{n+1} - 2d + 3 \leq c\,2^{n+1} - d$. **(#)**

Isolating d in (#), we get $d \geq 3$. **(**)**

Finally, we choose c and d so that (*) and (**) are satisfied.
For example, we can pick $d = 3$ and $c = 10$. □