Notes on Induction and Recursion

Jayadev Misra
The University of Texas at Austin

November 17, 2009

Contents

1 Introduction

Let us try to prove the following identity for all n, $n \geq 1$:

$1 + 2 + \ldots + n = \frac{n \times (n+1)}{2}$.

Let us start by verifying this identity for some small values of n.

- $n = 1$: $1 = \frac{1 \times 2}{2}$.
- $n = 2$:

$$\begin{array}{ll} & 1 + 2 \\ = & \{\text{arithmetic}\} \\ & 3 \\ = & \{\text{arithmetic}\} \\ & \frac{2 \times 3}{2} \end{array}$$

- $n = 3$:

$$\begin{array}{ll} & 1 + 2 + 3 \\ = & \{\text{let us try something different: from the last proof}\} \\ & \frac{2 \times 3}{2} + 3 \\ = & \{\text{arithmetic}\} \\ & \frac{3}{2} \times (2 + 2) \\ = & \{\text{arithmetic}\} \\ & \frac{3 \times 4}{2} \end{array}$$

Can we write such a proof for $n + 1$ instead of 3? If we could then (1) we will have to justify replacing $1 + 2 + \ldots + n$ by $\frac{n \times (n+1)}{2}$, and (2) we will have to show: $\frac{n \times (n+1)}{2} + (n + 1) = \frac{(n+1) \times (n+2)}{2}$. The second part is easy

$$\begin{array}{ll} & \frac{n \times (n+1)}{2} + (n + 1) \\ = & \{\text{arithmetic}\} \end{array}$$

$$
\begin{array}{ll}
 & \frac{(n+1)}{2}(n+2) \\
= & \{\text{rewriting}\} \\
 & \frac{(n+1)\times(n+2)}{2}
\end{array}
$$

The first part is exactly what the induction principle allows us to assume.

2 Induction Over Natural Numbers

Let $P.n$ be a proposition that includes n, a natural number, as a free variable. The following principle can be used to prove $(\forall n :: P.n)$.

- Prove $P.0$, and
- prove $(\forall i : i \geq 0 : P.i \Rightarrow P.(i+1))$.

The justification for the above rule – known as the induction principle over natural numbers – is as follows. First, we have a proof of $P.0$; next from $P.0 \Rightarrow P.1$, we have $P.1$; .., from $P.i \Rightarrow P.(i+1)$ we have a proof of $P.(i+1)$, for all i, $i \geq 0$.

3 Examples

3.1 Example from Arithmetic

Show that $4^{n+2} + 5^{2n+1}$ is divisible by 21, for all n, $n \geq 0$.

$n = 0$: $4^{0+2} + 5^{2\times 0+1} = 16 + 5$ is divisible by 21.

$n+1$ assuming the result holds for n: Substituting $n+1$ for n in the formula:

$$
\begin{array}{ll}
 & 4^{n+3} + 5^{2n+3} \\
= & \{\text{Arithmetic}\} \\
 & 4 \times 4^{n+2} + 5^2 \times 5^{2n+1} \\
= & \{\text{Factoring}\} \\
 & 4 \times [4^{n+2} + 5^{2n+1}] + 21 \times 5^{2n+1}
\end{array}
$$

The first term is divisible by 21, by induction hypothesis and the second term because it is a multiple of 21.

3.1.1 Fibonacci Numbers

Fibonacci numbers are defined as follows.
$F.0 = 0$, $F.1 = 1$, and $\langle \forall i : i \geq 0 : F.(i+2) = F.i + F.(i+1) \rangle$.
Show that for any n, $n \geq 0$, $(+i : 0 \leq i < n : F.i) < F.(n+1)$.

- $n = 0 : (+i : 0 \leq i < 0 : F.i) = 0 < F.1$.
- $n + 1$, where $n \geq 0$:

$$
\begin{array}{ll}
 & (+i : 0 \leq i < n+1 : F.i) \\
= & \{\text{Arithmetic}\} \\
 & (+i : 0 \leq i < n : F.i) + F.n \\
< & \{\text{Induction Hypothesis}\} \\
 & F.(n+1) + F.n \\
= & \{\text{Definition of Fibonacci}\} \\
 & F.(n+2)
\end{array}
$$

Exercise Show that $F.n < 2^n$.

3.1.2 Harmonic numbers

Harmonic numbers are defined as follows:

$$H_n = 1/1 + 1/2 + 1/3.. + 1/n.$$

Show that $\sum_{i=1}^{n} H_i = (n+1)H_n - n$.
We will have to start the induction from $n = 1$.

- $n = 1$: $H_1 = 1 = (1+1)H_1 - 1$.
- $n > 1$:

$$
\begin{array}{ll}
 & \sum_{i=1}^{n} H_i \\
= & \{\text{arithmetic}\} \\
 & \sum_{i=1}^{n-1} H_i \ + H_n \\
= & \{\text{Induction Hypothesis}\} \\
 & nH_{n-1} - (n-1) + H_n \\
= & \{\text{Arithmetic}\} \\
 & n(H_{n-1} + 1/n) - n + H_n \\
= & \{\text{Arithmetic}\} \\
 & nH_n + H_n - n \\
= & \{\text{Arithmetic}\} \\
 & (n+1)H_n - n
\end{array}
$$

It is easy to show that the harmonic series diverges, i.e., there is no bound such that all H_n fall below that bound. We will show that

$H_{2^k} > k/2$, for all k, $k \geq 0$.

The base case, $k = 0$, is easy. For the inductive case,

$$
\begin{array}{ll}
 & H_{2^{k+1}} \\
= & \{\text{definition of } H\} \\
 & H_{2^k} + \sum_{i=2^k+1}^{2^{k+1}} 1/i \\
\geq & \{\text{each term in the sum is at least } 1/(2^{k+1}) \text{ and there are } 2^k \text{ terms}\} \\
 & H_{2^k} + 2^k \times 1/(2^{k+1}) \\
= & \{\text{simplify the second term}\}
\end{array}
$$

$$
\begin{array}{ll}
 & H_{2^k} + 1/2 \\
> & \{\text{induction hypothesis}\} \\
 & k/2 + 1/2 \\
= & \{\text{arithmetic}\} \\
 & (k+1)/2
\end{array}
$$

3.2 Tiling with Trimino

Given is a checker board having $2^n \times 2^n$ squares, $n \geq 0$; one square is declared to be *open* and the remaining ones are *closed* squares. A *trimino* covers exactly 3 squares. Show that it is possible to tile the board with triminos such that each closed square is covered by exactly one trimino (and triminos cover only closed squares).

Exercise Show that $2^n \times 2^n - 1$ is divisible by 3, for all n, $n \geq 0$, i.e, the claim stated above is feasible.

Proof of the claim is by induction on n.

- $n = 0$: the number of squares to be tiled is $2^0 \times 2^0 - 1 = 0$. Hence a trivial tiling exists.
- $n + 1$, $n \geq 0$: Partition the board into 4 equal subboards of size $2^n \times 2^n$. One of the subboards contains the open square. For each of the remaining subboards call the corner square that is closest to the center of the checker board *ajar*. Inductively, each subboard can be tiled, where we treat each ajar square as an open square. Finally the ajar squares can be tiled with one trimino.

3.3 A Domino Tiling Problem

Given is a chess board that has an even number of rows, say $2 \times M$ where $M \geq 1$, and any number of columns N, $N > 1$. An arbitrary black cell and a white cell are designated *open*; the remaining cells are *closed*. Cover the chess board with 2×1 dominoes in such a way that every closed cell is covered by exactly one domino and open cells are not covered.

Call two cells *neighbors* if they share an edge. Define a *path* to be a sequence of cells where adjacent cells are neighbors. A path is *even* if it has an even number of cells.

Observation: An even path can be covered by dominoes.

Proof: Each pair of adjacent cells in the path being neighbors belong to the same row or same column. Therefore, any pair of adjacent cells can be covered by a single domino. Starting from the first cell in the path cover every pair by a domino, and since the path is even all cells can be covered.

Note: A board that has an even number of cells can be covered.

We prove the main result by induction on M, the number of rows divided by two[1].

• Case $M = 1$: The board has two rows. The closed cells form one even path if the open cells are adjacent; they form two even paths if the open cells are non-adjacent. In either case, the open cells can be covered, using the observation.

• Case $M > 1$: divide the board into 2 subboards: the *upper* board consists of the two top rows and the *lower* one consists of the remaining rows. If the two open cells are in upper then, from the case $M = 1$, upper can be covered. And, lower can be covered since it has an even number of cells. If the two open cells are in lower then upper can be covered, because it has an even number of cells, and lower can be covered inductively. So, we next consider the case when one of the open cells is in upper and the other is in lower.

Assume that the open cell in upper is white. Pick a black cell, B, in the second row of upper —this choice is possible because there are at least two columns— and an adjacent cell, W, in lower —which is guaranteed to be white. Declare both these cells to be open. Now, upper can be covered, using the argument for the case $M = 1$, and lower can be covered inductively. Next use a single domino to cover the B,W cells.

3.4 A Pebble Movement Game

Consider a row consisting of $2n + 1$ cells, $n \geq 0$. The center cell is empty; each of the n cells to its left has a black pebble and each cell to the right has a white pebble. It is given that: (1) a pebble can be moved to a neighboring cell if it empty, and (2) a pebble can jump over another pebble to land in a cell that is empty. It is required to show that all the black and white pebbles can be interchanged.

We formalize the problem as follows. Given is a string over the alphabet $\{x, y, e\}$; here x is a black pebble, y is a white pebble and e denotes the empty cell. Initially, the string is $x^n e y^n$. Let $P \sim Q$ denote that string P can be transformed to string Q by repeated applications of the rules of pebble movement. Clearly, $\sim$ is an equivalence relation. Henceforth, p and q denote single symbols, and P and Q are strings.

The rules of pebble movement are:

$$pe \sim ep \tag{R1}$$
$$pqe \sim eqp \tag{R2}$$

Our goal is to show that $x^n e y^n \sim y^n e x^n$. The following lemma is a generalization of (R1).

Lemma 1 $Pe \sim eP$.
Proof:: Proof is by induction on the length of P.

[1]The following proof is due to Sridhar Srinivasan, a student in CS 336 during Spring 2001.

• Case P is empty: We have to show $e \sim e$, which follows from the reflexivity of $\sim$.

• Inductive Case: $pPe \sim epP$

$$\begin{array}{ll} & pPe \\ \sim & \{\text{Induction hypothesis: } Pe \sim eP\} \\ & peP \\ \sim & \{\text{R1: } pe \sim ep\} \\ & epP \end{array}$$

Note that in transforming Pe to eP, the number of applications of (R1) is exactly the length of P.

Exercise: Why can't induction hypothesis be used —instead of R1— in the last step of the above proof?

We now a prove a more general result than $x^n e y^n \sim y^n e x^n$, the original result we had intended to prove. We show that any arrangement of pebbles of any number of colors can be transformed to any of its permutations; we assume that there is one empty cell. In symbols, we show that any string consisting of a single e can be transformed to any permutation.

We prove this result by showing that any two adjacent symbols can be transposed. The result follows from (R1) if either of the symbols is e. Otherwise, without loss in generality, assume that the configuration contains a substring $pqRe$, where R is a string. We show that pq can be transposed to qp, i.e., $pqRe \sim qpRe$.

$$\begin{array}{ll} & pqRe \\ \sim & \{\text{Lemma 1: } Re \sim eR\} \\ & pqeR \\ \sim & \{\text{Rule R2: } pqe \sim eqp\} \\ & eqpR \\ \sim & \{\text{Lemma 1: } eqpR \sim qpRe\} \\ & qpRe \end{array}$$

Note that this proof does not explicitly use induction; induction is buried within Lemma 1.

This result does not give an explicit procedure for transforming $x^n e y^n$ to $y^n e x^n$ (though, undoubtedly, you can specify a series of adjacent transpositions to accomplish this goal). Now, we give an explicit procedure for transforming PeQ to QeP.

Lemma 2 $peQ \sim Qep$
Proof:: Proof is by induction on n, the length of Q.

• $n = 0$: $pe \sim ep$ follows from (R1).

• $n > 0$: Let $Q = qR$.

$$
\begin{array}{ll}
 & peQ \\
= & \{Q = qR\} \\
 & peqR \\
\sim & \{\text{Rule R1: } pe \sim ep\} \\
 & epqR \\
\sim & \{\text{Rule R2: } epq \sim qpe\} \\
 & qpeR \\
\sim & \{\text{induction: } peR \sim Rep\} \\
 & qRep \\
= & \{Q = qR\} \\
 & Qep
\end{array}
$$

We can compute the number of steps (each step is an application of R1 or R2) required to transform peQ to Qep by this procedure. Let $S(n)$ be the number of steps where $n = |Q|$. From the proof given above, $S(0) = 1$ and $S(n+1) = 2+S(n)$, because there is one application each of (R1) and (R2) and application of induction on a string that is one less than the size of the original. Solving, $S(n) = 2n + 1$.

Lemma 3 $PeQ \sim QeP$
Proof:: Proof is by induction on m, the length of P.

- $m = 0$: $eQ \sim Qe$ follows from Lemma 1.
- $m = 1$: $peQ \sim Qep$ follows from Lemma 2.
- $m > 1$: Let $P = Rp$.

$$
\begin{array}{ll}
 & PeQ \\
= & \{P = Rp\} \\
 & RpeQ \\
\sim & \{\text{Lemma 2: } peQ \sim Qep. \text{ Takes } 2n+1 \text{ steps.}\} \\
 & RQep \\
\sim & \{\text{Lemma 1: } Qe \sim eQ. \text{ Takes } n \text{ steps.}\} \\
 & ReQp \\
\sim & \{\text{induction on } ReQ\text{: } ReQ \sim QeR\} \\
 & QeRp \\
= & \{P = Rp\} \\
 & QeP
\end{array}
$$

We count the number of steps for transformation as given by this proof. Let $T(m, n)$ be the number of steps where $m = |P|$ and $n = |Q|$. Then,

$T(0, n) = n$, as given by the first case in the proof.
$T(1, n) = 2n + 1$, as given by the second case in the proof.
$T(m + 1, n) = T(m, n) + 3n + 1$, from the third case in the proof.

Solving the equations, $T(0,n) = n$ and $T(m,n) = 3mn + m - n$, for $m > 0$. Switching the roles of P and Q, we get another procedure that takes $3mn - m + n$ steps, for $n > 0$. Therefore,

$T(m,0) = m$, $T(0,n) = n$
$T(m,n) = 3mn + \min(m-n, n-m)$, for $m > 0$ and $n > 0$

For $m = n$, $T(m,n) = 3mn$.

Exercise The given proof does not give an optimal procedure for transformation. Show that $xxeyy$ can be transformed to $yyexx$ in 10 steps (our procedure takes $3 \times 2 \times 2 + 2 - 2 = 12$ steps.

Solution

$x(xeyy) \overset{T(1,2)=5}{\sim} xyyex \sim xyeyx \sim eyxyx \sim yexyx \sim yyxex \sim yyexx$

3.5 Winning Strategy in Finite Games

A finite game, such as tic tac toe, can be represented by a finite tree in which every leaf node is labelled + (a win for the first player) or − (a win for the second player). An internal node is labelled + if there is a winning strategy for the first player at that node; similarly, a node is labelled − if there is a winning strategy for the second player. That is, an internal node is labelled + if either (1) it is a move for the first player at that node and there is a son of this node labelled +, or (2) it is a move for the second player and all sons are labelled +. Similarly, a label of − is defined.

Show that the root node can be labelled + or −, i.e., every finite game has a winning strategy for one of the players.

We show that every node can be labelled + or −. The proof is by induction on the height of that node: leaf has height 0 and the height of a node is one more than the highest height of a son. Consider a node all of whose sons have been labelled. If it is a move for the first player at this node then: either (1) there is a son labelled +: in that case, the node may be labelled +, or (2) all sons are labelled −: in that case the node may be labelled −.

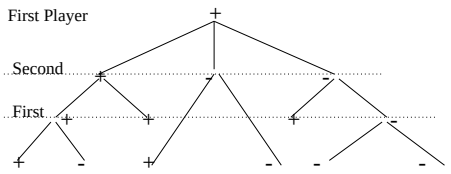

Figure 1: Winning Strategies in a Finite Game

3.6 Totality of Functions

An arbitrary recursive definition of a function may be circular, and hence, the function may not be *well-defined*. Induction can be used to show that certain functions over natural numbers are well-defined.

First, we show that the factorial function is well-defined. The factorial is defined as follows.

$fac(0) = 1$
$fac(n+1) = n \times fac(n)$

We show that for all n, "$fac(n)$ is defined". Let $P.n$ be "$fac(n)$ is defined".

- $n = 0$: $fac(0)$ is well-defined, from the function description.
- $n = 1$, $n \geq 0$: from the induction hypothesis, $fac(n)$ is well-defined; hence $n \times fac(n)$, or $fac(n+1)$ is well-defined.

Consider the *Ackermann* function. It is defined as follows over a pair of natural numbers.

$A(0, n) = n + 1$
$A(m, 0) = A(m-1, 1)$, $m \neq 0$
$A(m, n) = A(m-1, A(m, n-1))$, $m \neq 0, n \neq 0$

It is not possible to show that A is well-defined using induction on natural numbers. We will use induction on well-founded sets to prove this result. What needs to be shown is that *every* call to A in the rhs of a definition has arguments that are smaller than the arguments in the lhs. Thus, we have to show that $(m-1, 1) < (m, 0)$ and $(m-1, A(m, n-1)) < (m, n)$ and $(m, n-1) < (m, n)$. To see that the last check is needed, replace $A(m, n-1)$ by $A(m, n)$; the definition is then circular.

Exercise Show that $A(n, n) \geq 2^n$, $n \geq 0$.

3.7 Connectivity in a Butterfly Network

Show that there is a unique path between any pair of input-output nodes in a butterfly network.

Description of a butterfly network A butterfly network of size N, where $N = 2^n$, for some n, $n \geq 0$, has $n+1$ stages numbered 0 through n. For $n = 0$ the butterfly network consists of a single node in stage 0. Henceforth, we take $n > 0$. Each stage has N nodes; the nodes are uniquely indexed by an n-bit string. Nodes in stage 0 are called input nodes and those in stage n are output nodes. Each node except those in stage 0 has two input ports, known as *top* and *bottom*. Each node except in the last stage has two output ports known as

top and *bottom*. The output ports of nodes in stage i are connected to the input ports of nodes in stage $i+1$, $0 \leq i < n$, as follows.

For a node x in stage i let its index be written in the form pqr where p is a bit string of length i, q is a single bit and r is the remaining portion (of length $n-i-1$) of the index; note that p or r, or both, could be empty. Node x is connected to nodes with indices $p0r$ and $p1r$ in the following stage. If $q = 0$ then both outputs of x link to the top ports and if $q = 1$ then both outputs of x link to the bottom ports. (The exact connection of top and bottom ports is irrelevant for proving the result of this paper.)

Solution Consider a node x in stage i, $0 \leq i \leq n$. An input node whose index matches the last $n-i$ bits of x is called a *tip* of x. Specifically, if the index of x is of the form uv where u is of length i then a tip of x has an index of the form wv. Thus the only tip of an input node is itself, and each output node has all input nodes as tips. A stage i node has 2^i different tips. Call a node a non-tip of x if it not a tip of x. We show,

Theorem: For any node x, there is a unique path from any tip of x to x, and there is no path from a non-tip of x to x.

Proof: Proof is by induction on the stage of x. If the stage is 0, the result is straightforward. Consider a node x in stage $i+1$ whose two predecessors (in stage i) are y and z. Observe that (1) the set of tips of y and z are disjoint, and (2) a tip of x is a tip of y or z (but not both because of 1). By induction hypothesis, every tip of y has a unique path to y, and no path to z (being a non-tip of z). Thus, every tip of y has a unique path to x; similarly, for the tips of z. Hence, every tip of x has a unique path to x. A non-tip of x is a non-tip of both y and z, and from the induction hypothesis, has path to neither. Therefore, a non-tip of x has no path to x.

3.8 Bit propagation

Let $X_0, .., X_{N-1}$ be boolean variables where N is a power of 2. In each step, every X_i is set to $X_i \oplus X_{i+1}$, where $\oplus$ is "exclusive or", or addition modulo 2, and $+$ is addition modulo N. We show that eventually all X_i become 0. Let $X_{(i,k)}$ be the value of the i^{th} bit after k steps.

Theorem $X_{(i,k+2^j)} = X_{(i,k)} \oplus X_{(i+2^j,k)}$, for all $k, j \geq 0$ and $0 \leq i < N$.
Proof:: is by induction on j.

- $j = 0$:
  left side $= X_{(i,k+1)}$, which is $X_{(i,k)} \oplus X_{(i+1,k)}$.
  right side $= X_{(i,k)} \oplus X_{(i+1,k)}$.
- $j + 1$:

$$\begin{array}{ll} & X_{(i,k+2^{j+1})} \\ \Rightarrow & \{\text{rewriting}\} \end{array}$$

$$
\begin{array}{ll}
 & X_{(i,k+2^j+2^j)} \\
\Rightarrow & \{\text{Induction}\} \\
 & X_{(i,k+2^j)} \oplus X_{(i+2^j,k+2^j)} \\
\Rightarrow & \{\text{Induction on each term}\} \\
 & X_{(i,k)} \oplus X_{(i+2^j,k)} \oplus X_{(i+2^j,k)} \oplus X_{(i+2^{j+1},k)} \\
\Rightarrow & \{\text{Property of } \oplus\} \\
 & X_{(i,k)} \oplus X_{(i+2^{j+1},k)}
\end{array}
$$

Corollary $X_{iN} = 0$, for all i, $0 \leq i < N$.

Proof:: Let $N = 2^n$. Setting k to 0 and j to n the theorem yields

$$
\begin{array}{l}
X_{iN} \\
= X_{i,0+2^n} \\
= X_{i,0} \oplus X_{i+2^n,0} \\
= X_{i,0} \oplus X_{i,0} \\
= 0
\end{array}
$$

Exercise: For integers j, k, $0 \leq j < N$, $0 \leq k < N$, define $j \sqsubseteq k$ if every bit in the binary expansion of j is at most the corresponding bit in k. Show that $X_{(i,k)} = \langle \oplus j : j \sqsubseteq k : X_{(i+j,0)} \rangle$.

Hint: Use induction on k. In the inductive step, let $k = s + 2^r$, where $s < 2^r, r \geq 0$.

A Variation of Bit Propagation Let $X_0, .., X_{N-1}$ be integer variables where N is a power of 2. In each step every X_i is set to $|X_i - X_{i+1}|$, where $+$ is addition modulo N.

Theorem All variables become 0 eventually.
Proof:: After the first step all variables are non-negative. We start our argument by assuming that all variables are non-negative. Let M be the maximum value of any X_i. Observe that the maximum value never increases in a step. Proof of the theorem is by induction on M. If M is 0 then the result follows. For $M > 0$, we apply the following inductive argument.

A step sets the last bit of X_i – call it b_i – to $b_i \oplus b_{i+1}$, where $\oplus$ is addition modulo 2. Using the previous result, eventually all b_is become 0, i.e., all numbers are even. Let Y_i be $X_i/2$ at this point. Since the maximum of X_is is at most M, $M > 0$, the maximum of the Y_is is less than M. Executing some steps with the X_is is same as executing the same number of steps with Y_is and then multiplying the result by 2. Using induction the Y_is become eventually 0; hence, with the original values the variable values become 0 eventually.

4 Complete Induction

Complete Induction, also known as *The Second Principle of Induction*, or *Strong induction* allows us to assume that $P.0, P.1, \ldots, P.n$ all hold in proving $P.(n+1)$.

Theoretically, this principle is no stronger than the original version you have seen; any proof using complete induction can be converted to a proof using the original form of induction. Sometimes, it is convenient to use this form.

Example Show that any number above 11 can be written as a sum of 4's and 5's.

• Proof using complete induction: First show that 12, 13 and 14 can be so represented. For any number $n+1$, $n \geq 14$, there is a representation for $n-3$ using complete induction; add a 4 to this representation to get one for $n+1$.

• Proof using the original form of induction: Number 12 is a sum of three 4's. For any number $n+1$, $n \geq 12$, consider two cases: (1) the representation of n includes a 4, in that case replace the 4 by a 5 to get a representation for $n+1$, (2) the representation of n does not include a 4; therefore it has to include at least three 5's (since $n \geq 12$); replace three 5's by four 4's.

5 Strategies in Applying Induction

5.1 Strengthening

Consider proving $(+i : 0 \leq i < n : 2^{-i}) \neq 2$.

A proof by induction may be attempted as follows.

- $n = 0$: $(+i : 0 \leq i < 0 : 2^{-i}) = 0 \neq 2$.
- $n+1$: $(+i : 0 \leq i < n+1 : 2^{-i}) = (+i : 0 \leq i < n : 2^{-i}) + 2^{-n}$.

By induction hypothesis, the first term in the above expression differs from 2. However, that is not sufficient to show that the sum differs from 2.

In such cases, we look for a stronger result that is amenable to proof by induction. For this example, we prove:
$(+i : 0 \leq i < n : 2^{-i}) = 2 \times (1 - 2^{-n})$.
Then the required result follows because for any n, $n \geq 0$, $(1 - 2^{-n}) \neq 1$ and, hence, $2 \times (1 - 2^{-n}) \neq 2$.

Here is a way to prove this result using induction.

Example : $(+i : 0 \leq i < n : 2^{-i}) \neq 2$.

- $n = 0$: trivial
- $n+1$:

$$\begin{array}{ll} & 2^{-0} + ... + 2^{-(n+1)} \\ = & \{\text{Arithmetic}\} \\ & 2^{-0} + 2^{-1} \times [2^{-0} + ... + 2^{-n}] \\ \neq & \{\text{Induction Hypothesis}\} \end{array}$$

$$
\begin{array}{ll}
 & 1 + 1/2 \times 2 \\
= & \{\text{Arithmetic}\} \\
 & 2
\end{array}
$$

5.2 Pay Attention to the base case

Consider the following "proof" of $x^n = 1$, for any positive real x and any natural n.

- $n = 0$: $x^0 = 1$.
- $n + 1$:

$$
\begin{array}{ll}
 & x^{n+1} \\
= & \{\text{Arithmetic}\} \\
 & \frac{x^n \times x^n}{x^{n-1}} \\
= & \{\text{Induction}\} \\
 & (1 \times 1)/1 \\
= & \{\text{Arithmetic}\} \\
 & 1
\end{array}
$$

The proof is incorrect in replacing x^{n-1} by 1, because for $n = 0$, x^{n-1} has not been shown to be 1.

5.3 Proof by Contradiction

A proof by contradiction can often be replaced by a proof by induction. A typical proof by contradiction is: let n be the smallest natural number that violates $P.n$. We display m, $m < n$, such that $P.m$ is violated. The proof by contradiction establishes – note that there is often no need to assume that n is the smallest –

$$\neg P.n \Rightarrow (\exists m : m < n : \neg P.m).$$

Thus, the same proof establishes by contrapositive,

$$(\forall m : m < n : P.m) \Rightarrow P.n.$$

which is a proof by induction, see complete induction in page 12. Observe that for $n = 0$, this reads $true \Rightarrow P.0$, which is the premise of the induction hypothesis.

5.4 Misapplication of Induction

We prove that the shortest curve between any two points in a plane is a straight line. Let x, y be two points in a plane, not necessarily distinct, and let d be the straight-line distance between x, y. The proof is by induction on d.

For $d = 0$, $x = y$. Then any curve other than a straight-line has higher distance.

For $d > 0$, let z be a point midway along the shortest curve between x, y. The distance along the shortest curve is $\leq d$; hence the distance along the shortest curve between x, z and between z, y is each $\leq d/2$. Applying induction, the shortest curves between x, z and between y, z are straight lines. Now, using triangle inequality, $|xz| + |yz| \geq |xy|$, i.e., $|xz| + |yz| \geq d$. Since $|xz| \leq d/2$ and $|zy| \leq d/2$, this is satisfiable only if $|xz|$ and $|zy|$ are both $d/2$, i.e., z falls on the straight line xy.

This proof is wrong; you can't apply induction on real numbers (d in this example).

6 Induction Exercises

1. Binomial Theorem: Prove the following version of the binomial theorem.

$$(1+x)^n = \sum_{i=0}^{n} \left(\begin{array}{c} n \\ i \end{array} \right) x^i$$

   Hint: Use the following facts about the binomial coefficients.

$$\left(\begin{array}{c} n \\ 0 \end{array} \right) = \left(\begin{array}{c} n \\ n \end{array} \right) = 1$$

   Also, for $0 < i \leq n$:

$$\left(\begin{array}{c} n+1 \\ i \end{array} \right) = \left(\begin{array}{c} n \\ i \end{array} \right) + \left(\begin{array}{c} n \\ i-1 \end{array} \right)$$

2. Prove the following identities using induction.
   (a) $\sum_{i=0}^{n} i = \frac{n \times (n+1)}{2}$.
   (b) $\sum_{i=0}^{n} \frac{i \times (i+1)}{2} = \frac{n \times (n+1) \times (n+2)}{6}$.
   (c) $\sum_{i=0}^{n} i^2 = \frac{n \times (n+1) \times (2n+1)}{6}$.
   (d) $\sum_{i=0}^{n} i^3 = \frac{n^2 \times (n+1)^2}{4}$.
   (e) $\sum_{i=0}^{n} r^i = \frac{r^{n+1}-1}{r-1}$, $r \neq 1$.
   (f) $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$.
   (g) $(1+x)^n \geq 1 + nx$, for $n \geq 0$, provided $1 + x \geq 0$.

Solution: For the inductive case,

$$\begin{array}{ll} & (1+x)^{n+1} \\ = & \{\text{properties of exponents}\} \\ & (1+x) \times (1+x)^n \\ \geq & \{\text{given: } 1+x \geq 0\text{; inductive hypothesis: } (1+x)^n \geq 1+nx\} \\ & (1+x) \times (1+nx) \\ = & \{\text{arithmetic}\} \\ & 1+x+nx+nx^2 \\ \geq & \{nx^2 \geq 0\text{, because } n \geq 0 \text{ and } x^2 \geq 0\} \\ & 1+(n+1) \times x \end{array}$$

3. Let x and y be real numbers. Define $f^0(x,y) = (x,y)$ and for any natural i, $f^{i+1}(x,y) = f^i((x+y)/2, (x-y)/2)$. Show that $f^{2\times n}(x,y) = (x/2^n, y/2^n)$, for all natural n.

4. For positive integers p, q and natural r show that

   $$\gcd(2^p - 1, 2^q + 1) = \gcd(2^p - 1, 2^{r\times p+q} + 1)$$

   Prove the result by induction on r. Use the following fact about gcd.

   $\gcd(x,y) = \gcd(x, n \times x + y)$, for positive integers x, y and natural n.

   Solution: The result holds trivially for $r = 0$. For any r, $r \geq 0$,

   $$\begin{array}{ll} & \gcd(2^p - 1, 2^{(r+1)\times p+q} + 1) \\ = & \{\text{arithmetic}\} \\ & \gcd(2^p - 1, 2^{p+r\times p+q} + 1) \\ = & \{\text{rewriting the second argument}\} \\ & \gcd(2^p - 1, 2^{r\times p+q} \times (2^p - 1) + 2^{r\times p+q} + 1) \\ = & \{\text{fact about gcd. Let } x = 2^p - 1,\ y = 2^{r\times p+q} + 1,\ n = 2^p - 1\} \\ & \gcd(2^p - 1, 2^{r\times p+q} + 1) \\ = & \{\text{induction}\} \\ & \gcd(2^p - 1, 2^q + 1) \end{array}$$

5. Write $m|n$ to mean that m divides n. Show that

   For all natural p, $3^{p+1} | (2^{3^p} + 1)$

   Solution: Proof is by induction on p.

   • $p = 0$: $3|(2^1 + 1)$

   • $p + 1,\ p \geq 0$: We have to show $3^{p+2} | 2^{3^{(p+1)}} + 1$.

   Abbreviate 2^{3^p} by x. Then, $2^{3^{(p+1)}} = 2^{3^p \times 3} = (2^{3^p})^3 = x^3$.

$$
\begin{array}{ll}
 & 3^{p+1}|(x+1) \\
\Rightarrow & \{p \geq 0\} \\
 & 3|(x+1) \\
\Rightarrow & \{\text{arithmetic}\} \\
 & 3|((x+1)^2 - 3 \times x) \\
\equiv & \{\text{expanding the dividend}\} \\
 & 3|(x^2 - x + 1) \\
\Rightarrow & \{3^{p+1}|(x+1)\} \\
 & (3 \times 3^{p+1})|((x+1) \times (x^2 - x + 1)) \\
\Rightarrow & \{\text{arithmetic}\} \\
 & (3 \times 3^{p+1})|(x^3 + 1) \\
\Rightarrow & \{\text{rewriting } x\} \\
 & 3^{p+2}|(2^{3^{(p+1)}} + 1)
\end{array}
$$

6. (Generalization of the previous exercise) Show that $3^{p+1}|(2^q + 1)$, for all natural p, and q of the form $3^{p(2\times t+1)}$.

   Hint: Solution is similar to the previous one. 2^q plays the role of x. Increasing p by 1 gives q^3.

7. (Three-halves conjecture) There is a famous open problem in mathematics, known as the three-halves conjecture, which goes as follows.

   Given any positive integer n apply the following steps repeatedly until n becomes 1. If n is odd then set n to $(3 \times n + 1)/2$; if n is even set it to $n/2$. Show that this procedure terminates for every n.

   This conjecture has been verified for many values of n. However, there is no proof yet. Show that if this procedure terminates for t then it terminates for $2^p \times (t+1)/3^p - 1$, for every p, $p \geq 0$, provided the given expression denotes a positive integer. Prove the result by induction on p.

8. (Three-halves conjecture) Show that there is no infinite increasing chain.

   Solution: Consider an infinite increasing chain. Every element of the chain is odd (an even element is followed by a strictly smaller element) and different from 1. (Number 1 can appear only as part of a finite chain).

   For two adjacent elements $2 \times s + 1$ and $2 \times t + 1$, we show that

   - s is odd, and
   - $t = (3 \times s + 1)/2$

   Therefore, corresponding to any infinite increasing chain there exists another infinite increasing chain whose elements are strictly smaller than the corresponding elements of the first chain. Applying this argument repeatedly, we can show an increasing infinite chain which contains 1, a contradiction.

$$
\begin{array}{ll}
 & 2 \times t + 1 = (3 \times (2 \times s + 1) + 1)/2 \\
\Rightarrow & \{\text{arithmetic}\}
\end{array}
$$

$$
\begin{array}{ll}
 & 2 \times t + 1 = 3 \times s + 2 \\
\Rightarrow & \{\text{arithmetic}\} \\
 & t = (3 \times s + 1)/2
\end{array}
$$

In order for t to be integer, s is odd.

9. (A generalization of the previous result) A sequence $x_0,\ x_1, \ldots x_n$, $n > 1$, is an n-upchain if each x_i, except possibly x_n, is odd and greater than 1, and $x_{i+1} = (3 \times x_i + 1)/2$, $0 \leq i < n$. Show that $x_0 \geq 2^n - 1$.

   Solution: Proof is by induction on n.

   $n = 1$ and $n = 2$: The smallest odd number appearing as x_0 is 3; so the result holds for these two cases trivially.

   $n + 1,\ n \geq 2$: Consider the first n numbers in the chain. Each such x_i is odd. Moreover, $x_0 > 3$, because 3 starts an upchain of length 2 only. Hence, each x_i is of the form $2 \times y_i + 1$, where $y_i > 1$. The sequence $y_0 \ldots y_n$ is an n-upchain, following the argument given in the previous exercise. Hence, $y_0 \geq 2^n - 1$, or $x_0 = 2 \times y_0 + 1 \geq 2^{n+1} - 1$.

10. Show that the sum of the interior angles of a convex n-gon is $180(n - 2)$ degrees.

11. Consider a full binary tree (where each internal node has exactly two children). The *size* of the tree is the number of its leaf nodes. The *weight* of a node is defined as follows: (1) for a leaf node it is 1, and (2) for an internal node, it is the product of the sizes of its two subtrees (rooted at its children). Show that the sum of the node weights for any binary tree is a function only of its size (and independent of its shape).

    Hint: The sum of the node weights for a tree of size n is $n(n + 1)/2$.

12. A tournament among 2^n players is arranged as a perfect binary tree. There are n rounds numbered 1 through n; the winner of a round i match advances to round $i+1$, and the (unique) winner of round n is the champion.

    Prize money is distributed as follows. The champion receives 1 unit (1 unit is approximately \$1.4 million for 2007 Wimbledon Tennis Tournament), and the loser in the final match receives $1/2$ unit. A loser in round i, $1 \leq i < n$, receives half as much as a loser in round $i + 1$. What is the total amount of prize money distributed?

    Solution: Total prize money is $1 + 1/2 \times n$. You can see this directly, as follows. The prize money received by a loser in round i is 2^{-n-1+i}, and round i has 2^{n-i} losers. So, the losers in round i receive $2^{-n-1+i} \times 2^{n-i} = 1/2$ units. Since there are n rounds, the total received by all losers is $1/2 \times n$. And the champion receives 1 unit. So, the total prize money is $1 + 1/2 \times n$.

    For an inductive proof, consider the money spent on all except the first round losers. Inductively, it is $1 + 1/2 \times (n - 1)$. And, the losers in round

1 each receive 2^{-n} units and there are 2^{n-1} of them. So the total spent on the first round losers is 1/2 unit. $1/2 + 1 + 1/2 \times (n-1) = 1 + 1/2 \times n$.

13. For distinct integers x, y and natural n, $x - y$ divides $(x^n - y^n)$, for all n, $n \geq 0$.

    Hint: Write $(x^{n+1} - y^{n+1})$ as $x^{n+1} - xy^n + xy^n - y^{n+1}$. Factor the first two terms and the last two.

14. Show that there is a solution to the Towers of Hanoi problem.

15. What is

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n ?$$

16. Show that for $n > 1$ the following expression is irrational.

$$\underbrace{\sqrt{1 + \sqrt{1 + \ldots}}}_{n \text{ } 1s}$$

17. Show that

    (a) $n^3 - n$ is divisible by 3.

    (b) Sum of the cubes of any 3 consecutive integers is divisible by 9.

    (c) $13^n + 6$ is divisible by 7, for even n.

    (d) for n greater than 7, $n = 3 \times \alpha + 5 \times \beta$, for some integers α, β.

18. Let $x_0 = 1$, and $x_{n+1} = x_n + 1/x_n$, for $n \geq 0$. Show that for all n, $n \geq 1$, $x_n > \sqrt{n}$.

    Solution We show the equivalent result: $x_n^2 > n$. Prove the base case, $x_1^2 > 1$, from $x_1 = x_0 + 1/x_0$. For $n \geq 1$, we show $x_{n+1}^2 > n + 1$.

$$\begin{array}{ll} & x_{n+1}^2 \\ > & \{\text{inductively, } x_n > \sqrt{n}. \text{ Hence, } x_n > 0. \\ & \quad x_{n+1} = x_n + 1/x_n;\ x_{n+1} > x_n\} \\ & x_{n+1} \times x_n \\ = & \{\text{expanding } x_{n+1}\} \\ & (x_n + 1/x_n) \times x_n \\ = & \{\text{algebra}\} \\ & x_n^2 + 1 \\ > & \{\text{induction hypothesis}\} \\ & n + 1 \end{array}$$

19. The following algorithm can be used to determine if an integer, given in decimal notation, is divisible by 11. Starting from the right end of the number alternately add and subtract the digits; for example 154 gives $4 - 5 + 1$, i.e. 0. The number is divisible by 11 iff the computed result is 0. Prove the correctness of this procedure.

Solution: Let function $asum$ applied to an integer give the result of alternate addition and subtraction, as described above. More formally, for a digit d, $0 \leq d \leq 9$, and any positive integer n

$$asum(d) = d, \text{ and } asum(10 \times n + d) = d - asum(n)$$

For any integer m, we show that $m = asum(m) \pmod{11}$. The theorem follows as a corollary. When m is a single digit, the identity is easy to see since $m = asum(m)$. For the general case, let $m = 10 \times n + d$.

$$\begin{array}{ll} & m \bmod 11 \\ = & \{m = 10 \times n + d\} \\ & (10 \times n + d) \bmod 11 \\ = & \{\text{properties of mod}\} \\ & (10 \times n \bmod 11 + d \bmod 11) \bmod 11 \\ = & \{\text{properties of mod}\} \\ & (-n \bmod 11 + d \bmod 11) \bmod 11 \\ = & \{\text{induction hypothesis}\} \\ & (d \bmod 11 - asum(n) \bmod 11) \bmod 11 \\ = & \{\text{properties of mod}\} \\ & (d - asum(n)) \bmod 11 \\ = & \{\text{definition of } asum\} \\ & asum(10 \times n + d) \bmod 11 \\ = & \{m = 10 \times n + d\} \\ & asum(m) \bmod 11 \end{array}$$

20. Consider the equation $au = ub$ where a and b are symbols and u is an unknown finite string (over some alphabet). Show that there is a solution to this equation in u iff $a = b$.

21. There is a finite group of children where each child is *clean* or *dirty*. No child knows if it is clean or dirty, but it can see if every other child is clean or dirty. It is common knowledge that there is at least one dirty child.

    In a *round*, (1) the children are asked: do you know if you are dirty, and (2) each of them responds with "NO (I don't know)", "YES, I am dirty", or "YES, I am clean". Responses are heard by all children. Rounds are repeated ad infinitum starting at round 0.

    Prove that a child who sees n dirty children, $n \geq 0$, will answer YES in round n, but no earlier.

22. A couple (called host and hostess) invites 4 other couples to a party. Each person shakes some hands – possibly 0 – but no one shakes hands with his/her spouse. The host determines that the remaining people at the party have all shaken different numbers of hands. What is the number of hands shaken by the hostess?

Solution: Generalize the problem: N couples have been invited. Prove, by induction, that the hostess shakes N hands. Observe that The number of hands shaken by all except the host is 0 through $2 \times N$.

Claim 0: For $N = 0$, the hostess shakes 0 hands.

Next, consider $N > 0$. Call the person who shakes $2 \times N$ hands $2N$ and, similarly, 0 identifies the person who shook 0 hands. Let $x \sim y$ denote that x and y shake hands. For a set S, $x \sim S$ denotes that x shakes hands with all members of S. Let A denote all parties.

Claim 1: $2N \not\sim 0$: because 0 shakes no hand.

Claim 2: $2N \sim (A - \{2N, 0\})$: $2N$ does not shake hands with $2N$, and from Claim 2, does not shake with 0. Since $2N$ shakes $2 \times N$ hands, it shakes with all others.

Claim 3: $2N$ and 0 are spouses: None with whom $2N$ shakes hands is its spouse. Hence, from Claim 2, the spouse of $2N$ is either $2N$ —which is impossible— or 0.

Claim 4: Hostess is neither $2N$ nor 0: $2N$ and 0 are spouses. Since the host is neither of $2N$ or 0, the hostess is neither of $2N$ or 0.

After removing the couple $2N$ and 0 from the picture, we have an identical situation with $N-1$ couples: every one has shaken one less hand (because every remaining person has shaken with $2N$). Inductively, the hostess shakes $N - 1$ hands with these $N - 1$ couples. Since the hostess shakes with $2N$, she shakes N hands in all.

23. A *full* binary tree is a binary tree in which every internal node has exactly two children. Let b be the bag of pathlengths (to the leaves). Show that $\sum_{i \in b} 2^{-i} = 1$.

    Hint: Use induction on the size of b.

24. *Gray code* for n, $n > 0$, is a sequence which contains all n-bit words, with the property that adjacent words differ in exactly one bit position (here, the very first and the very last words are taken to be adjacent). For $n = 1$, a possible sequence is 0 1 and for $n = 2$, one possible sequence is 00 01 11 10. Show that the following recursive procedure correctly creates Gray code for any n, $n > 0$.

    Let S_n denote the Gray code sequence for n. Let S_1 be 0 1. For $n + 1$: take each word in S_n and append a 0 to its beginning, transforming each word to $n + 1$ bits; then, reverse the sequence of words in S_n and append 1 to the beginning of each word.

25. (A Property of Reflected Gray Code) The Gray code constructed in the last exercise has the following property. Take the sequence S_n, for any n, $n > 0$. For each pair of adjacent words, construct their longest common prefix. Show that the set of prefixes includes every word with fewer than n bits (exactly once). For example, S_2 is 00 01 11 10 and the set of prefixes

is $\{0, \epsilon, 1\}$, where ϵ is the 0-bit word; this set includes every 0-bit and 1-bit word.

7 Induction on Well-Founded Sets

A set W together with a binary relation $<$ is called well-founded if every chain in W is finite: a chain is a sequence of items from W – $x_0, .., x_i, ..$ – where, $x_{i+1} < x_i$, for all i. The items in the chain need not be distinct.

An equivalent definition of well-foundedness is: every non-empty subset of W has a minimal element. (An element x is *minimal* in set S if there is no element y in S such that $y < x$.)

Note: A minimal element x need not be smaller than the other elements of S.

It can be shown that the two definitions of well-foundedness are equivalent.

Examples:

- The set of natural numbers is well-founded under the less than relation, by applying the second definition.
- The integers are not well-founded under $<$, because – applying the second definition – we cannot display a minimal integer.
- A set in which $<$ is the empty relation is well-founded. Applying the second definition any element of a non-empty subset can be taken to be minimal.
- The set of finite strings over any alphabet (finite or infinite) are well-founded under prefix ordering, subsequence ordering, substring (contiguous subsequence) ordering, suffix ordering.
- The set of finite sets (over elements from some domain) are well-founded under subset ordering.

  Note: Infinite sets are not well-founded under subset ordering. Let $T_0 = \{0, 1, 2, ..\}$, $T_1 = \{1, 2, ...\}$, $T_i = \{i, i+1, ..\}$. Then, $T_{i+1} \subset T_i$. We have an infinite chain $T_0, T_1, ...$
- Tuples under lexicographic ordering: Let $<$ be a total order over some domain. For pairs (x, y) and (x', y') from that domain, define the lexicographic order as follows:
  $(x, y) \prec (x', y')$ means $(x < x') \vee (x = x' \wedge y < y')$.

  To see that this defines a well-founded order, take any chain. Mark off the points where the first component strictly decreases. Each segment (between mark offs) is finite because each corresponds to a chain in the original domain, and there are a finite number of segments, because the starting points of the segments define a chain in the original domain.

Exercise: Show that tuples with infinite number of components are not well-founded under lexicographic ordering.

Hint: Let the i^{th} tuple be $0^i 1^\omega$. Using $0 < 1$, the $(i+1)^{th}$ tuple $<$ the i^{th} tuple. We have, thus, constructed an infinite chain.

- Trees under subtree ordering.
- Finite strings under lexicographic ordering.
- if $(W_1, <_1)$ and $(W_2, <_2)$ are well-founded then so is $(W, <)$ where $W = W_1 \times W_2$, and $(x, y) < (x', y') \equiv x <_1 x' \wedge y <_2 y'$.
- The strings over the terminal and non-terminal symbols of a context-free grammar are well-founded under $<$ where $s < t$ denotes that $s \longrightarrow {}^* t$.

Exercise: Cartesian product of well-founded sets are well-founded.

Exercise: If $(W, <)$ is well-founded and $<'$ is a subrelation of $<$ then $(W, <')$ is well-founded. Thus, empty relation is well-founded.

Exercise: Let $(W, <)$ be well-founded. Suppose, $<'$ is a binary relation over W' and f is a function, $f : W' \longrightarrow W$ that respects $<$ (i.e., $x <' y \Rightarrow f.x < f.y$). Show that $(W', <')$ is well-founded.

Hint: Any infinite chain in W' maps to an infinite chain in W.

Exercise: Let $(W, <)$ be well-founded. Show that $<$ is irreflexive and anti-symmetric.

7.1 Induction Principle over Well-Founded Sets

Let $(W, <)$ be a well-founded set. Then, $P.x$ for all x in W can be shown by proving

$$
\begin{array}{l}
(\forall x : x \in W : \\
\quad (\forall y : y \in W,\ y < x : P.y) \Rightarrow P.x \\
).
\end{array}
$$

In words, if $P.x$ can be proven assuming that P holds for all elements "smaller" than x then P holds for all elements.

An important special case is induction over natural numbers:

$$
\begin{array}{l}
(\forall x : x \in \aleph : \\
\quad (\forall y : y \in \aleph,\ y < x : P.y) \Rightarrow P.x \\
).
\end{array}
$$

For $x = 0$, the requirement reduces to:

$$(\forall y : y \in \aleph,\ y < 0 : P.y) \Rightarrow P.x$$

which is equivalent to – because $(\forall y : y \in \aleph,\ y < 0 : P.y)$ is *true* since the range of quantification is empty – $P.0$. The requirement corresponding to the positive integers amounts to the "strong induction principle" over naturals.

7.2 Equivalence of two definitions of well-foundedness

Two different definitions of well-foundedness are given in the last section. We show here that the two definitions are equivalent.

- If W has an infinite chain then there is a subset that has no minimal element: take the elements of the infinite chain to form the subset.
- If there is a subset that has no minimal element then W has an infinite chain. We demonstrate an infinite sequence of elements $x_0, x_1, ..,$ where $x_{i+1} < x_i$, for all i. Pick any element of the subset, call it x_0. Since the subset has no minimal element, x_0 is not minimal; hence, there is an element x_1 in the subset such that $x_1 < x_0$. Applying this strategy over and over, an infinite chain can be constructed.

7.3 Examples

7.3.1 Termination

Show that the following program terminates. Here, no fairness is assumed in the choice of statements, and ? denotes an arbitrary natural number.

var x, y : natural
do[$x > 0 \ \rightarrow \ x, y := x - 1, ?$
[] $y > 0 \ \rightarrow \ y := y - 1$
]

It is sufficient to show that the pair (x, y) decreases lexicographically in each step. This result cannot be proven by induction over natural numbers since there is no bound on the number of steps to termination.

7.3.2 Ackermann

The Ackermann function was defined previously.

$A(0, n) = n + 1$
$A(m, 0) = A(m - 1, 1),\ m \neq 0$
$A(m, n) = A(m - 1, A(m, n - 1)),\ m \neq 0, n \neq 0$

We prove that for each (m, n), $A(m, n)$ has a value, i.e., the function is well-defined. Proof is by induction on the pairs (m, n) where we order the pairs lexicographically. For pairs of the form $(0, n)$ the function value is $n + 1$. For

all other (m, n), $m \neq 0$, the function has a value provided the function value is defined for pairs that are lexicographically smaller (observe that in each defining equation the arguments of the function in the right side are lexicographically lower than those in the left side).

7.3.3 A Fundamental theorem of Number Theory

The following theorem, due to Euclid, is fundamental in number theory. Given positive integers m and n, there exist integers p and q such that

$$p \times m + q \times n = \gcd(m, n).$$

We prove this result by induction on pairs of positive integers. Order such pairs lexicographically. We prove a more general base case than the case for the pair $(1, 1)$.

• $m = n$:

$$\begin{aligned} & 1 \times m + 0 \times n \\ = \; & m \\ = \; & \gcd(m, m) \end{aligned}$$

Thus, the theorem is established by letting $p, q = 1, 0$.

• Inductive Case: Assuming that the result holds for all pairs that are lexicographically smaller than (m, n), we prove the result for (m, n). If $m = n$ the result holds from the base case, above. Therefore, we need only consider $m \neq n$. Assume that $m > n$; the analysis is symmetric for $n > m$.

Consider the pair of positive integers $(m - n, n)$ which is lexicographically smaller than (m, n). By the induction hypothesis, there exist integers p', q' such that

$$\begin{aligned} & p' \times (m - n) + q' \times n = \gcd((m - n), n) \\ \Rightarrow \quad & \{m > n \Rightarrow [\gcd((m - n), n) = \gcd(m, n)]\} \\ & p' \times (m - n) + q' \times n = \gcd(m, n) \\ \Rightarrow \quad & \{\text{rewriting the lhs}\} \\ & p' \times m + (q' - p') \times n = \gcd(m, n) \end{aligned}$$

Letting $p, q = p', q' - p'$, we have established the result for (m, n).

Exercise: Prove this result by ordering pairs of positive integers by the magnitude of their sums.

Exercise: In the equation $p \times m + q \times n = \gcd(m, n)$, show that $p > 0 \equiv q \leq 0$.

Solution In the given equation both p and q can not be positive, because then the left side will exceed both m and n, and the right side is at most the minimum of m and n. Hence, if p is positive then q is non-positive, i.e.,

$$p > 0 \;\Rightarrow\; q \leq 0$$

By similar arguments, both p and q can not be non-positive, because then the left side is non-positive and the the right side, being a gcd, is always positive. Hence, if p is non-positive then q is positive, i.e.,

$$p \leq 0 \;\Rightarrow\; q > 0$$

Combining the two observations,

$$p > 0 \;\equiv\; q \leq 0$$

8 Structural induction

It is often the case that a structure (set, function, relation, data structure, circuit, language) is defined recursively, as shown below.

(basis) $a, b \in S$
(recursion) $x \in S \Rightarrow f(x) \in S$

It is assumed that nothing else belongs to S. Properties of S can be proven by induction as follows. To show that $P.x$ holds for every x in S, prove

(basis) $P.a$, $P.b$
(recursion) $P.x \Rightarrow P.(f(x))$

We can argue as follows about why this scheme works. To every element of S assign a *level*; elements a, b have level 0 and any other element in S has a level equal to the minimum number of applications of the recursive step to put that element in S. It follows that for any element x in S, (1) either $x = a$ or $x = b$, or (2) $x = f(y)$, for some y, where the level of y is less than that of x. we prove that $P.x$ holds for all elements x in S by induction on levels.

The induction principle shown above may be generalized to other kinds of recursive definitions, as shown in some of the examples below.

8.1 A Context-free Language

Consider the context-free grammar

$$S \;\longrightarrow\; ab \mid aSb \mid SS$$

Show that every string in this language has equal number of as and bs. Prove this statement as follows:

(basis) Show the result for ab.
(induction) assume the result for S and show it for aSb.
(induction) assume the result for S_1, S_2 and show it for S_1S_2.

It is instructive to look at a more difficult property of these strings: for any string x in this language, the number of as at any *point* in x is at least the number of bs at that point. For example, consider the string $aababb$, and verify the given property at every point in this string. To prove the result by induction:

(basis) Show the result for 3 possible points in ab.
(induction) assume the result for S and show it for aSb.
(induction) assume the result for S_1, S_2 and show it for S_1S_2.

8.2 The One-Third Problem

Given a set of reals S where,

(basis) $0 \in S$, $1 \in S$.
(recursion) $x \in S \wedge y \in S \Rightarrow (x+y)/2 \in S$.

Show that $1/3 \notin S$. We prove the proposition, $S \subseteq \{m/2^n \mid m, n \text{ naturals}, n \geq 0,\ 0 \leq m \leq 2^n\}$. Clearly, the proposition holds in the base case, because $0 = 0/2^0$ and $1 = 1/2^0$. Next, for any two elements of S, say $m_1/2^{n_1}$ and $m_2/2^{n_2}$, the element they generate – $1/2(m_1/2^{n_1} + m_2/2^{n_2}) = \frac{2^{n_2} \times m_1 + 2^{n_1} \times m_2}{2 \times (2^{n_1+n_2})}$ – is also of this form. Hence, $1/3 \notin S$ because $1/3 = m/2^n$ has no solution in naturals m, n.

Exercise: Show that $S = \{m/2^n \mid m, n \text{ naturals}, n \geq 0,\ 0 \leq m \leq 2^n\}$.

Hint: Prove that $m/2^n \in S$ where $n \geq 0 \wedge 0 \leq m \leq 2^n$, by induction n.

8.3 Stack Languages

Consider a stack of length N, $N \geq 1$, that is used to convert an input string to an output string as follows. At any step, either (1) the next symbol from the input string is pushed onto the stack (provided there is room in the stack), or (2) the top symbol of the stack is removed and appended to the end of the output string (provided the stack is non-empty). We define $X\ R.N\ Y$ – where $R.N$ is a binary relation over sequences X, Y – to mean that Y is a possible output sequence of a stack of size N given X as the input sequence.

For $N \geq 0$, the relation $R.N$ is given by

- $\epsilon\ R.N\ \epsilon$
- $X\ R.N\ X'\ ,\ Y\ R.(N+1)\ Y' \ \Rightarrow\ aXY\ R.(N+1)\ X'aY'$

where a is any arbitrary data item. The second rule states that given an input string aXY to a stack of size $N+1$, the item a appears in the output at some

point. Prior to output of a, item a is at the bottom of the stack and hence, the stack behaves as if its size is N in converting some portion of the input, X, to X'. Following the output of a, the stack is empty and hence the remaining input sequence Y is converted to Y' using a stack of size $N + 1$.

Several interesting properties—using induction on the length of X—can be proven about this relation.

For $N = \infty$, let $R.N$ be R. Then,

- $\epsilon \; R \; \epsilon$
- $X \; R \; X' \; , \; Y \; R \; Y' \; \Rightarrow \; aXY \; R \; X'aY'$

8.4 Well-Founded Ordering over Bags

Let $(D, <)$ be a well-founded set. For finite bags X, Y over D define

$$Y \subset X \; \equiv \; \langle (A \neq \phi \; \wedge \; (\forall y : y \in B : \langle \exists x : x \in A : y < x \rangle) \rangle,$$
where $A = X - Y$ and $B = Y - X$.

We may imagine that Y is constructed from X by removing the elements in A and adding the elements in B. It is required that some element be removed ($A \neq \phi$) and each element that is added be smaller than some removed element. We can show that finite bags are well-founded under the $\subset$ relation.

8.5 Loosely-Coupled Processes

8.6 Powerlist

9 Recursive Algorithms

9.1 gcd; binary gcd

9.2 Tower of Hanoi

9.3 Isolating defective coins

There are 3^n, $n > 0$, coins out of which one coin is lighter than others. Using a balance, isolate the defective coin in n weighings.