Noetherian Induction

Andreas Klappenecker

Let $(A, \preceq)$ be a partially ordered set. The relation $a \preceq b$ can be read as "a precedes b". For elements a and b in A, we write $a \prec b$ if and only if $a \preceq b$ and $a \neq b$ holds. For notational convenience, we also write $a \succeq b$ if and only if $a \preceq b$ holds, and $a \succ b$ if and only if $a \prec b$ holds.

We call $(A, \preceq)$ a **well-founded set** if and only if every non-empty subset M of A contains at least one minimal element m with respect to the order relation $\preceq$. Put differently, any non-empty subset M of a well-founded set A contains an element m such that there does not exist an element m' in M satisfying $m' \prec m$.

An **infinite descending chain** S in a partially ordered set $(A, \preceq)$ is an totally ordered subset of A without minimal element. In other words, S contains elements $a_1, a_2, \dots$ such that $a_1 \succ a_2 \succ a_3 \succ \cdots$.

Proposition 1. *Let $(A, \preceq)$ be a partially ordered set. Then the following two statements are equivalent:*

(i) $(A, \preceq)$ *is a well-founded set.*

(ii) There does not exist any infinite descending chain in A.

Proof. (i) $\Rightarrow$ (ii). Seeking a contradiction, we assume that (i) holds but that there exists an infinite descending chain S in A. However, S is a non-empty subset of A without minimal element, contradicting the fact that A is a well-founded set.

(ii) $\Rightarrow$ (i). Seeking a contradiction, we assume that (ii) holds, but that A is not a well-founded set. Therefore, there exists a non-empty subset C of A that does not contain a minimal element. However, a non-empty set that does not contain a minimal element must contain an infinite descending chain, contradicting our assumption (ii). $\square$

Theorem 1 (The Principle of Noetherian Induction)**.** *Let $(A, \preceq)$ be a well-founded set. To prove that a property $P(x)$ is true for all elements x in A it is sufficient to prove the following two properties:*

(a) ***Induction basis:*** *$P(x)$ is true for all minimal elements of A.*

(b) ***Induction step:*** *For each non-minimal x in A, if $P(y)$ is true for all $y \prec x$, then $P(x)$ is true.*

Remark. Instead of checking the two conditions (a) and (b) of the previous theorem, it suffices to prove a single condition:
(a&b) For all x in A, if $P(y)$ is true for all $y \prec x$, then $P(x)$ holds.
If x is minimal in A, then there are no elements y preceding x, so condition *(a&b)* requires us to prove that $P(x)$ is true. Thus, *(a&b)* is simply a slick way

to write (a) and (b) in a concise form, but the proof requires the same amout of work.

Proof. Seeking a contradiction, we assume that the set of counter examples

$$C = \{x \in A \mid P(x) \text{ is false}\}$$

is not empty. Since A is a well-founded set, there must exist a minimal element m of C. By construction, all elements a in A such that $a \prec m$ satisfy $P(a)$ is true, hence $P(m)$ must be true, contradicting our assumption that C is not empty. $\square$

Examples of Well-Founded Sets

Let us take a look at a few examples of well-founded sets.

Example 2. Let $\mathbf{N} = \{1, 2, \dots\}$ denote the set of natural numbers. Then $(\mathbf{N}, \leq)$ with the familiar "less than or equal to" relation $\leq$ is a well-founded set, since there obviously cannot exist an infinite decreasing chain in $\mathbf{N}$.

Example 3. Let L be an integer. The set $\{x \in Z \mid x \geq L\}$ with the "less than or equal to" relation $\leq$ is a well-founded set.

Counterexample 4. The set of integers $\mathbf{Z}$ with the "less than or equal to" relation $\leq$ is a totally ordered set, but is **not** a well-founded set.

Example 5. Let $A = \{S \in P(\mathbf{N}) \mid |S| < \infty\}$ be the set consisting of the finite subsets of the set of natural numbers. Then $(A, \subseteq)$ with the usual set inclusion is a partially ordered set. Since any set S in A of cardinality n can have at most n predecessors, there cannot exist an infinite descending chain in A. Therefore, $(A, \subseteq)$ is a well-founded set.

Let $(A, \preceq)$ be a partially ordered set. The **lexicographic ordering** $\sqsubseteq$ on $A \times A$ is given by

$$(a, b) \sqsubseteq (a', b') \text{ if and only if } \begin{cases} a \prec a', \\ a = a' \text{ and } b \preceq b', \end{cases}$$

for all a, b, a', b' in A.

Proposition 6. *Let $(A, \preceq)$ be a partially ordered set. If $(A, \preceq)$ is a well-founded set, then the lexicographically ordered set $(A \times A, \sqsubseteq)$ is a well-founded set as well.*

Proof. Seeking a contradiction, we assume that there exists an infinite decreasing chain $S = \{(a_k, b_k) \mid k \in I\}$ in $(A \times A, \sqsubseteq)$. If the set $F = \{a_k \mid (a_k, b_k) \in S, k \in I\}$ of the first components of S is an infinite set, then F is an infinite decreasing chain in A, contradicting the fact that A is a well-founded set. Therefore, the set F must be finite. Since S is an infinite set, there must exist an a in F such that $L = \{b_k \mid (a, b_k) \in S, k \in I\}$ is an infinite set. Since S is an infinite decreasing chain, it follows that L must be an infinite decreasing chain in A, contradicting the fact that A is a well-founded set. Therefore, there does not exist any infinite decreasing chain S in $(A \times A, \sqsubseteq)$, which proves our claim. $\square$

Existence of Factorizations into Primes

The set $\mathbf{N}_2 = \{2, 3, \dots\}$ of integers greater than 1 is a well-founded set with respect to the usual "less than or equal" ordering relation $\leq$. Evidently, the number 2 is the only minimal element of $(\mathbf{N}_2, \leq)$. Furthermore, $\mathbf{N}_2$ is totally ordered with respect to $\leq$. It is not hard to see that $(\mathbf{N}_2, \leq)$ is a well-founded set. We can easily prove the existence of a factorization into primes using Noetherian induction.

Proposition 7. *Every integer $n \geq 2$ is a product of prime numbers.*

Proof. For $n \geq 2$, we let $P(n)$ denote the statement "n is a prime or a product of prime numbers". We need to show that $P(n)$ is true for all $n \geq 2$.

Induction basis: Since 2 is a prime, it follows that $P(2)$ is true.

Induction step: We assume that $n > 2$ and $P(n)$ is true for $2 \leq k < n$. If n is prime, the $P(n)$ is true. So assume that n is not prime, then $n = xy$ for some integers x and y in the range $2 \leq x < n$ and $2 \leq y < n$. By assumption $P(x)$ and $P(y)$ is true, so n is a product of primes, hence $P(n)$ is true.

It follows by induction that $P(n)$ is true for all $n \geq 2$. $\square$

Ackermann's Function

Let $\mathbf{N}_0 = \{0, 1, 2, \dots\}$ denote the set of non-negative integers. Consider the following recursively defined function

```
A(x,y) =
  if (x==0) then return y+1;
  else if (y==0) then return A(x-1,1);
       else return A(x-1,A(x,y-1));
```

This function is known as Ackermann's function. It is notorious for its extraordinary growth.

The function `A(x,y)` is defined for all inputs from $\mathbf{N}_0 \times \mathbf{N}_0$. One can show that `A(x,y)` defines a partial function, that is, its values are uniquely determined for those inputs where the function terminates. However, it is perhaps not apparent that the function actually is supposed to terminate for each input. In particular, any implementation will quickly run out of memory. Therefore, it does not seem obvious that `A(x,y)` defines a total function $\mathbf{N}_0 \times \mathbf{N}_0 \to \mathbf{N}_0$.

Proposition 8. *Ackermann's function* `A(x,y)` *is a total function that yields for each input $(x, y) \in \mathbf{N}_0 \times \mathbf{N}_0$ a non-negative integer value.*

Proof. Let $\sqsubseteq$ denote the lexicographic order on $\mathbf{N}_0 \times \mathbf{N}_0$, that is,

$$(m_1, m_2) \sqsubseteq (n_1, n_2) \text{ if and only if } \begin{cases} m_1 < n_1, \\ m_1 = n_1 \text{ and } m_2 \leq n_2. \end{cases}$$

Then $(\mathbf{N}_0 \times \mathbf{N}_0, \sqsubseteq)$ is a well-founded set with least element $(0, 0)$.

Induction basis: The value `A(0,0)` is defined and equal to 1.

Induction step: Let us assume that $A(m', n')$ is defined for all $(m', n') \sqsubset (m, n)$. Then we have the following three cases:

(a) If $m = 0$, then $A(0, n)$ is defined and equal to $n + 1$, since $A(0, y) = y + 1$.

(b) If $m \neq 0$ and $n = 0$, then $(m - 1, 1) \sqsubset (m, 0)$, so $A(m - 1, 1)$ is defined by induction hypothesis; hence $A(m, 0)$ is defined and equal to $A(m - 1, 1)$.

(c) If $m \neq 0$ and $n \neq 0$, then $(m, n - 1) \sqsubset (m, n)$, so $A(m, n - 1)$ is defined; furthermore, $(m - 1, y) \sqsubset (m, n)$ for all y in $\mathbf{N}_0$, so by induction hypothesis $A(m - 1, A(m, n - 1))$ is defined. However, this is precisely $A(m, n)$, so $A(m, n)$ is defined as well.

Therefore, the Ackermann function yields a nonnegative integer value for all inputs from $\mathbf{N}_0 \times \mathbf{N}_0$. $\square$