# 1 More on Induction

**Theorem 1.1**

Every integer greater than 1 is a product of primes.

*Proof.* For $n \in \mathbb{N}$, let $p(n) =$"n is a product of primes".

Let $n \in \mathbb{N}$ be arbitrary.

Suppose $n > 1$ and $\forall i \in \mathbb{N}.[1 < i < n$ IMPLIES $P(i)]$.

If $n$ is prime, then $n$ is a product of primes, and thus $P(n)$.

Otherwise, there are positive integeres $1 < k < n$, $1 < m < n$ such that $n = k \cdot m$.

By the inductive hypothesis, $k$ and $m$ are products of primes: $P(k)$ and $P(m)$.

Thus, $n = k \cdot m$ is a product of primes.

Therefore, for all $n \in \mathbb{N}$, and hence $(n > 1)$ IMPLIES $p(n)$. □

# 2 Recursively Defined Sets

Recursive definitions have 2 parts:

- a base case, that does not depend on anything else
- a constructor case, that depends on previous cases.

**Example 2.1**

1. Let $\{0, 1\}^*$ be a set of all finite strings of bits.

   Base Case: $\lambda$, empty string of length 0, is in $\{0, 1\}^*$.

   Constructor Case: If $s \in \{0, 1\}^*$, then $s0$ and $s1$ are in $\{0, 1\}^*$.

   Similarly, for any set $\Sigma$, $\Sigma^*$ is the of all finite length strings of letters from $\Sigma$.

2. Let $B$ be a set of finite strings of matched brackets.

   Base Case: $\lambda$, empty string of zero matched brackets, is in $B$.

   Constructor Case: if $p, q \in B$, then $p[q] \in B$.

3. Let $S$ be a set of syntactically correct formulas of propositional logic.

   Base Case: propositional variables are in $S$.

   Constructor Case: if $p, q \in S$, then NOT $p \in S$, $p$ AND $q \in S$, $p$ OR $q \in S, \ldots$

4. Let $M$ be a set of syntactically correct monotone formulas of propositional logic.

   Base Case: propositional variables are in M

   Constructor Case: if $p, q \in M$, then NOT $p \in M$, $p$ AND $q \in M$, $p$ OR $q \in M, \ldots$

   Note that $M$ is hte smallest set of formulas containing all the propositional variables and closed under AND and OR .

# 3 Structural Induction

Structural induction can be used to prove properties about recursively defined sets.

To prove $\forall s \in S.p(s)$, where $p : S \to \{T, F\}$ is a predicate, prove the following:

- $p(s)$ for all base cases $s$ given by the definition of $S$.
- $p(s)$ for the constructor cases $s$ given by the definition of $S$, assuming $p$ is true for the components of $s$.

**Example 3.1**

For all $f \in M$, let $V(f)$ be the number of occurrences of propositional variables in $f$ and let $B(f)$ be the number of occurrences of binary connectives in $f$.

Let $p(f) =$ "$N(f) = B(f) + 1$".

Base Case: If $f$ is a propositional variable, then $N(f) = 1 + B(f) = 1$, so $p(f)$ is true.

Constructor Cases: Consider $f = f'$ OR $f''$.

Assume $p(f')$ and $p(f'')$. Then $N(f) = N(f')+N(f'')$ and $B(f) = B(f')+B(f'')+1$.

By inductive hypothesis, $N(f) = (B(f')+1)+(B(f'')+1) = (N(f')+N(f'')+1)+1 = N(f) + 1$. So $p(f)$.

Similarly, if $f = f'$ AND $f''$, then $P(f)$ is true.

By structural induction, $\forall f \in M.p(f)$.

**Example 3.2**

$\mathbb{N}$ can be defined recursively.

Base Case: $0 \in \mathbb{N}$.

Constructor Case: if $n \in \mathbb{N}$, then $n + 1 \in \mathbb{N}$.

$\forall m \in \mathbb{N}.\forall n \in \mathbb{N}.p(m, n)$

Let $m \in \mathbb{N}$ be arbitrary.

Prove that $\forall n \in \mathbb{N}.p(m, n)$ by induction or generalisation.

$\forall m \in \mathbb{N}.\forall n \in \mathbb{N}.p(m, n)$ by generalisation.

Otherwise, define $\mathbb{N} \times \mathbb{N}$ recursively as follows:

1. Base Case: $(0, 0) \in \mathbb{N} \times \mathbb{N}$.
2. Constructor Case: If $(m, n) \in \mathbb{N} \times \mathbb{N}$, then $(m + 1, n), (m, n + 1) \in \mathbb{N}$.

Then assume $p(i, j)$ for all $(i, j)$, where $i \leq m$ or $j \leq n$, and either $i < m$ or $j < n$. Then prove $p(m, n)$.