1 Motivation

- Informal proof techniques permit the implicit use of general domain knowledge to simplify the proof of a conjecture for the given domain.

- Proofs by exhaustion are in most cases simple to perform but can only be applied for rather small numbers of objects.

- Very often a property has to be proven for an infinite sequence of objects, e.g. for all positive integers.
  - For all positive integers \( n > 1 \), the sum of all smaller positive integers is less than \( n^2 \).

- Direct proofs, proofs by contraposition, and proofs by contradiction allow to prove properties of infinite sequences. Often, however, it is hard to find such a proof since the property has to be proven for all objects simultaneously.

2 Mathematical Induction

- Mathematical induction uses the middle ground between exhaustive proof (object by object) and direct proofs (all objects simultaneously) by proving each object separately using an iterative proof.

- First principle of mathematical induction:
  - Prove the property for a start element using a proof by exhaustion, and then prove using a direct proof (or a proof by contraposition of contradiction) that if the property holds for an arbitrary object \( n \) in the sequence, then it also holds for the subsequent object \( n + 1 \).
  - Intuition: If you can get to the start line and can always do another step ahead, then you can do an infinite number of steps and get as far as you want.
  - Basis step: Prove \( P(1) \)
    Inductive hypothesis: \( P(n) \)
    Inductive step: prove that \( P(n) \rightarrow P(n + 1) \)
This proves each object individually without requiring an infinite number of steps. 
\[ P(1) \land (\forall x)(P(x) \to P(x + 1)) \to (\forall x)P(x) \]

\[ P(1), P(1) \to P(2), P(2), P(2) \to P(3), P(3), \ldots \]

- Note: The inductive hypothesis does not really assume that the initial conjecture is true. Rather it assumes that an arbitrary object has the property (which has already been proven for one object) and then introduces the implication \( P(n) \to P(n + 1) \) into the proof. The inductive hypothesis is thus similar to the temporary hypothesis used in predicate logic.

- Examples:

  * For all positive integers \( n > 1 \), the sum of all smaller positive integers is less than \( n^2 \).
    
    **Basis step:** prove for \( n = 2 \)
    
    \[ \sum_{k=1}^{1} k = 1 < 2^2 \]
    
    **Inductive hypothesis:** \( \sum_{k=1}^{n-1} k < n^2 \)
    
    **Inductive step:** prove \( P(n) \to P(n + 1) \)
    
    \[ \sum_{k=1}^{(n+1)-1} k = \sum_{k=1}^{n-1} k + n < n^2 + n < n^2 + 2n + 1 = (n + 1)^2 \]
    
    Therefore \( \sum_{k=1}^{n-1} k < n^2 \) for all \( n > 1 \)

  * \( 2^n - 1 \) is divisible by 3 for all even, positive integers.

  * Hint: Mathematical induction is performed over a sequence of objects, not necessarily the positive integers. To bring it into the standard form it might be necessary to renumber the elements.

  * The sum of all square numbers less than \( n^2 \) is less than \( n^3 \).
    
    - To match the pattern of the first principle of mathematical induction we can redefine this problem in terms of the the \( n^{th} \) square number: The sum of the first \( n - 1 \) square numbers is less than \( n^3 \).

  * Every odd length palindrome has an odd number of occurrences of exactly one symbol.
    
    - **Basis step:** All palindromes of length 1 have exactly one symbol and thus an odd number of occurrences of exactly one symbol.
    
    - **Inductive hypothesis:** All palindromes with odd length \( n \) have an odd number of occurrences of exactly one symbol.
    
    - **Inductive step:** Palindrome of length \( n + 2 \) \( s = btb \) where \( t \) is a palindrome of length \( n \).
      
      **Case 1:** \( b \) is the only symbol that occurs an odd number of times in \( t \). Then \( b \) is the only symbol that occurs an odd number of times in \( s \).
      
      **Case 2:** \( b \) occurs an even number (or 0 times) in \( t \). Then \( b \) occurs an even number of times in \( s \) and every element that occurs an odd number of times in \( t \) occurs also an odd number of times in \( s \).

  * For every odd integer \( n > 5 \), the sum of the previous 4 odd integers is \( 4n - 12 \).

  * Hint: In problems involving strings or similar structures, the objects are often ordered by the length of the string or the size of the structure and induction is performed using this partial ordering.
In some situations it is not possible to prove the existence of a property for a specific element \( n \) by only looking at the previous element in the sequence.

In a proof using mathematical induction we prove for one element at a time. At the time the property is proven for element \( n \) it is thus already proven for element 1\(... (n - 1) \).

Second principle of mathematical induction:

- Prove the property for a start element using a proof by exhaustion, and then prove using a direct proof (or a proof by contraposition of contradiction) that if the property holds for objects 1\(...n \) in the sequence, then it also holds for the subsequent object \( n + 1 \).

- Basis step: Prove \( P(1) \)
  Inductive hypothesis: \((\forall k)((k \leq n) \rightarrow P(k))\)
  Inductive step: prove that \((\forall k)((k \leq n) \rightarrow P(k)) \rightarrow P(n + 1)\)
  * This proves each object individually without requiring an infinite number of steps. 
    \[ P(1) \land (\forall x)((\forall k)((k \leq x) \rightarrow P(k)) \rightarrow P(x + 1)) \rightarrow (\forall x)P(x) \]
    \[ P(1), P(1) \rightarrow P(2), P(2), (P(1) \land P(2)) \rightarrow P(3), P(3), ... \]

- Examples:
  * Every integer \( n > 1 \) is a prime number or the product of prime numbers.
    - Basis step: \( n = 2 \) is a prime number.
    - Inductive hypothesis: All integers \( 1 < k \leq n \) are prime numbers or the product of prime numbers.
    - Inductive step:
      Case 1: \( n + 1 \) is prime.
      Case 2: \( n + 1 \) is not prime.
      If \( n + 1 \) is not prime, then \( n + 1 = m \star l, m, l < n + 1 \). Since \( n + 1 \) is the product of \( m \) and \( l \) and \( m \) and \( l \) are either prime numbers or the product of prime numbers, \( n + 1 \) is the product of prime numbers.
  * Any well formed expression involving only addition has an even number (or 0) parentheses.
    - Basis step:
      The shortest well formed expression involving only addition is \( x \) where \( x \) is an arbitrary variable, constant, or number. This involves 0 parentheses.
    - Inductive hypothesis: All well formed expressions involving only addition that contain at most \( n \) additions have an even number (or 0) parentheses.
    - Inductive step: Prove that if the inductive hypothesis holds, then all well formed expressions of this form which contain \( n + 1 \) additions also have an even number (or 0) parentheses.
      To prove this we have to look at all possible expressions of this kind. Well formed expressions \( u \) involving \( n + 1 \) additions can be formed in the following ways:
      Case 1: \( u = s + t \) where \( s \) and \( t \) together contain \( n \) additions.
Since $s$ and $t$ each have an even number (or 0) parentheses and the number of parentheses in $u$ is equal to the sum of the parentheses in $s$ and $t$, $u$ has an even number (or 0) parentheses.

Case 2: $u = (s + t)$ where $s$ and $t$ together contain $n$ additions. Since $s$ and $t$ each have an even number (or 0) parentheses and the number of parentheses in $u$ is equal to the sum of the parenthesis in $s$ and $t + 2$, $u$ has an even number of parentheses.

* You can form any positive integer $n \geq 4$ by adding 2s and 5s.

- Hint: The second principle of mathematical induction is a generalization of the first principle. In some situations both can be applied but one of them leads to a simpler problem formulation.