Mathematics for Computer Science

Prof. dr.hab. Viorel Bostan

Technical University of Moldova

viorel.bostan@adm.utm.md

Pre Lecture 5

Well Ordering Principle

Use WOP to prove propositions on predicates:

$$P(n) \text{ is true } \forall n \in \mathbb{N}.$$

Well Ordering Principle

Use WOP to prove propositions on predicates:

$$P(n) \ \text{ is true } \forall n \in \mathbb{N}.$$

1. Define the set C, set of counterexamples to P being true:

$$C = \{n \in \mathbb{N} \mid P(n) \ \text{ is false } \}.$$

Well Ordering Principle

Use WOP to prove propositions on predicates:

$$P(n) \text{ is true } \forall n \in \mathbb{N}.$$

1. Define the set C, set of counterexamples to P being true:

$$C = \{n \in \mathbb{N} \mid P(n) \text{ is false } \}.$$

2. By contradiction assume that C is nonempty.

Well Ordering Principle

Use WOP to prove propositions on predicates:

$$P(n) \text{ is true } \forall n \in \mathbb{N}.$$

1. Define the set C, set of counterexamples to P being true:

$$C = \{n \in \mathbb{N} \mid P(n) \text{ is false }\}.$$

2. By contradiction assume that C is nonempty.
3. By Well Ordering Principle, there will be a smallest element $n \in C$.

Well Ordering Principle

Use WOP to prove propositions on predicates:

$$P(n) \text{ is true } \forall n \in \mathbb{N}.$$

1. Define the set C, set of counterexamples to P being true:

$$C = \{n \in \mathbb{N} \mid P(n) \text{ is false } \}.$$

2. By contradiction assume that C is nonempty.
3. By Well Ordering Principle, there will be a smallest element $n \in C$.
4. Reach a contradiction — often by showing how to use n to find another member of C that is smaller than n.

Well Ordering Principle

Use WOP to prove propositions on predicates:

$$P(n) \text{ is true } \forall n \in \mathbb{N}.$$

1. Define the set C, set of counterexamples to P being true:

$$C = \{n \in \mathbb{N} \mid P(n) \text{ is false }\}.$$

2. By contradiction assume that C is nonempty.
3. By Well Ordering Principle, there will be a smallest element $n \in C$.
4. Reach a contradiction — often by showing how to use n to find another member of C that is smaller than n.
5. Conclude that C must be empty, that is, no counterexamples exist.

Theorem

Every positive integer greater than one can be factored as a product of primes.

Proof.

Proof by WOP.

Well Ordering Principle

Theorem

Every positive integer greater than one can be factored as a product of primes.

Proof.

Proof by WOP.

Let C be the set of integers greater than one, that can not be factored as a product of primes.

Well Ordering Principle

Theorem

Every positive integer greater than one can be factored as a product of primes.

Proof.

Proof by WOP.
Let C be the set of integers greater than one, that can not be factored as a product of primes.

Assume that C is not empty. We will reach a contradiction.

Theorem

Every positive integer greater than one can be factored as a product of primes.

Proof.

Proof by WOP.
Let C be the set of integers greater than one, that can not be factored as a product of primes.

Assume that C is not empty. We will reach a contradiction.

If $C \neq \emptyset$, then there is the smallest element $n \in C$ by WOP.

Well Ordering Principle

Theorem

Every positive integer greater than one can be factored as a product of primes.

Proof.

Proof by WOP.
Let C be the set of integers greater than one, that can not be factored as a product of primes.

Assume that C is not empty. We will reach a contradiction.

If $C \neq \emptyset$, then there is the smallest element $n \in C$ by WOP.

Number n cannot be prime, since in this case n will be a product (of length one) of primes.

Theorem

Every positive integer greater than one can be factored as a product of primes.

Proof.

Proof by WOP.
Let C be the set of integers greater than one, that can not be factored as a product of primes.

Assume that C is not empty. We will reach a contradiction.

If $C \neq \emptyset$, then there is the smallest element $n \in C$ by WOP.

Number n cannot be prime, since in this case n will be a product (of length one) of primes.

Thus, n is not prime: $n = a \cdot b$, where $1 < a, b < n$.

Theorem

Every positive integer greater than one can be factored as a product of primes.

Proof.

Proof by WOP.
Let C be the set of integers greater than one, that can not be factored as a product of primes.

Assume that C is not empty. We will reach a contradiction.

If $C \neq \emptyset$, then there is the smallest element $n \in C$ by WOP.

Number n cannot be prime, since in this case n will be a product (of length one) of primes.

Thus, n is not prime: $n = a \cdot b$, where $1 < a, b < n$.

Since a and b are smaller than the smallest element in C, it follows that $a, b \notin C$.

Proof contd.

$n = a \cdot b$, where $1 < a, b < n$ and $a, b \notin C$.

Proof contd.

$n = a \cdot b$, where $1 < a, b < n$ and $a, b \notin C$.
Therefore, a and b can be written as a product of primes:

$$a = p_1 p_2 \dots p_k, \quad b = q_1 q_2 \dots q_s.$$

Proof contd.

$n = a \cdot b$, where $1 < a, b < n$ and $a, b \notin C$.
Therefore, a and b can be written as a product of primes:

$$a = p_1 p_2 \dots p_k, \quad b = q_1 q_2 \dots q_s.$$

Thus,

$$n = a \cdot b = p_1 p_2 \dots p_k \cdot q_1 q_2 \dots q_s.$$

and n is written as a product of primes.

Proof contd.

$n = a \cdot b$, where $1 < a, b < n$ and $a, b \notin C$.
Therefore, a and b can be written as a product of primes:

$$a = p_1 p_2 \dots p_k, \quad b = q_1 q_2 \dots q_s.$$

Thus,

$$n = a \cdot b = p_1 p_2 \dots p_k \cdot q_1 q_2 \dots q_s.$$

and n is written as a product of primes.

On the other hand, initially n was such a number that can not be factored as a product of primes.

Contradiction!
Therefore, set C is empty, meaning that all positive integers greater than 1 can be factored as product of primes! $\square$