CSE 20: Discrete Mathematics

Daniele Micciancio

Spring 2018
So far:
- Propositional Logic (logical connectives, etc.)
- Predicate Logic (quantifiers, etc.)
- Formal proofs (inference rules, etc.)

Today:
- Informal proofs
- Catalog of informal proof methods
- Some Theorems in Number Theory
- Reading: All of Chapter 1 + Chap 4.1
Formal proofs:
- easy to check, mechanical
- not always easy to “understand”
- still useful to justify informal proof methods

Informal proof:
- high level, fewer details
- convey intuition, not just correctness
- missing details should be easy to fill in
- still, mathematical and precise
Theorem: Every integer is even or odd

Is the theorem precise enough?
**Theorem:** Every integer is even or odd

Is the theorem precise enough?

**Definition:** An integer $n$ is even is $n = 2m$ for some integer $m$. An integer $n$ is odd if $n = 2m + 1$ for some integer $m$. 

**Theorem:** Every integer is even or odd

Is the theorem precise enough?

**Definition:** An integer $n$ is even if $n = 2m$ for some integer $m$. An integer $n$ is odd if $n = 2m + 1$ for some integer $m$.

Universe of discourse: $\mathbb{Z}$, the set of all integers.

Predicates:

- **Even:** $E(n) \iff \exists m. n = 2m$
- **Odd:** $O(n) \iff \exists m. n = 2m + 1$

**Theorem:** $\forall n. (E(n) \lor O(n))$

**Proof:** ???
**Theorem:** Every integer is even or odd

Is the theorem precise enough?

**Definition:** An integer $n$ is even if $n = 2m$ for some integer $m$. An integer $n$ is odd if $n = 2m + 1$ for some integer $m$.

Universe of discourse: $\mathbb{Z}$, the set of all integers.

Predicates:
- Even: $E(n) \iff \exists m. n = 2m$
- Odd: $O(n) \iff \exists m. n = 2m + 1$

**Theorem:** $\forall n. (E(n) \lor O(n))$

**Proof:** ???

For now let us just assume it is true
How to prove an implication

**Theorem:** $p \implies q$

- Premise: $p$
- Conclusion: $q$

Often $p, q$ contain variables, with implicit **universal** quantification
How to prove an implication

**Theorem:** \( p \implies q \)

- **Premise:** \( p \)
- **Conclusion:** \( q \)

Often \( p, q \) contain variables, with implicit **universal** quantification

**Direct Proof:**

- Assume \( p \) is true
- Show that \( q \) is also true
Theorem: \( p \implies q \)

- Premise: \( p \)
- Conclusion: \( q \)

Often \( p, q \) contain variables, with implicit **universal** quantification

**Direct Proof:**

- Assume \( p \) is true
- Show that \( q \) is also true

**Proof by Contraposition:**

- Assume \( q \) is false
- Show that \( p \) is also false

Same as direct proof for contrapositive \( \neg q \implies \neg p \).
Theorem: If $n$ is even, then $n^2$ is also even.

\[ \forall n. E(n) \rightarrow E(n^2) \]

Proof:
1. Let $n$ be an arbitrary integer.
**Theorem:** If $n$ is even, then $n^2$ is also even.

$$\forall n. E(n) \rightarrow E(n^2)$$

**Proof:**

1. Let $n$ be an arbitrary integer.
2. We want to prove the implication $E(n) \rightarrow E(n^2)$
**Theorem**: If $n$ is even, then $n^2$ is also even.

$$\forall n. E(n) \rightarrow E(n^2)$$

**Proof:**

1. Let $n$ be an arbitrary integer.
2. We want to prove the implication $E(n) \rightarrow E(n^2)$
3. Assume $E(n)$ is true. We need to show that $E(n^2)$ is true.
Theorem: If $n$ is even, then $n^2$ is also even.

$$\forall n. E(n) \rightarrow E(n^2)$$

Proof:

1. Let $n$ be an arbitrary integer.
2. We want to prove the implication $E(n) \rightarrow E(n^2)$
3. Assume $E(n)$ is true. We need to show that $E(n^2)$ is true.
4. By definition of $E(n)$, $n = 2m$ for some integer $m$
Theorem: If $n$ is even, then $n^2$ is also even.

$$\forall n. E(n) \rightarrow E(n^2)$$

Proof:

1. Let $n$ be an arbitrary integer.
2. We want to prove the implication $E(n) \rightarrow E(n^2)$
3. Assume $E(n)$ is true. We need to show that $E(n^2)$ is true.
4. By definition of $E(n)$, $n = 2m$ for some integer $m$
5. Therefore, $n^2 = (2m)^2 = 4m^2 = 2(2m^2)$
**Theorem:** If $n$ is even, then $n^2$ is also even.

$$\forall n. E(n) \rightarrow E(n^2)$$

**Proof:**

1. Let $n$ be an arbitrary integer.
2. We want to prove the implication $E(n) \rightarrow E(n^2)$
3. Assume $E(n)$ is true. We need to show that $E(n^2)$ is true.
4. By definition of $E(n)$, $n = 2m$ for some integer $m$
5. Therefore, $n^2 = (2m)^2 = 4m^2 = 2(2m^2)$
6. So, $E(n^2)$ because $n^2 = 2m'$ for $m'$ equal to
Theorem: If \( n \) is even, then \( n^2 \) is also even.

\[ \forall n. E(n) \rightarrow E(n^2) \]

Proof:

1. Let \( n \) be an arbitrary integer.
2. We want to prove the implication \( E(n) \rightarrow E(n^2) \).
3. Assume \( E(n) \) is true. We need to show that \( E(n^2) \) is true.
4. By definition of \( E(n) \), \( n = 2m \) for some integer \( m \).
5. Therefore, \( n^2 = (2m)^2 = 4m^2 = 2(2m^2) \).
6. So, \( E(n^2) \) because \( n^2 = 2m' \) for \( m' \) equal to
Theorem: If $n$ is even, then $n^2$ is also even.

$$\forall n. E(n) \rightarrow E(n^2)$$

Proof:

1. Let $n$ be an arbitrary integer.
2. We want to prove the implication $E(n) \rightarrow E(n^2)$
3. Assume $E(n)$ is true. We need to show that $E(n^2)$ is true.
4. By definition of $E(n)$, $n = 2m$ for some integer $m$
5. Therefore, $n^2 = (2m)^2 = 4m^2 = 2(2m^2)$
6. So, $E(n^2)$ because $n^2 = 2m'$ for $m'$ equal to

(A) $m^2$; (B) $m^2 + 1$; (C) $2m^2$; (D) $2m^2 + 1$
**Theorem**: If $n^2$ is even, then $n$ is also even

First attempt (direct proof)

- Assume $n^2 = 2m$
- Need to show that $n = 2m'$ for some $m'$

Proof requires to find an appropriate integer $m'$. How can we give an expression for $m'$?

Second attempt (proof by Contraposition)

1. Assume $n$ is not even. Need to show that $n^2$ is not even.
2. Since $n$ is an integer, it must be odd, i.e., $n = 2m + 1$.
3. Therefore, $n^2 = (2m + 1)^2 = 4m^2 + 4m + 1 = 2(2m^2 + 2m) + 1$.
4. So, $n^2 = 2m' + 1$ is odd.
5. This proves that $n^2$ is not even.
**Theorem:** If $n^2$ is even, then $n$ is also even

First attempt (direct proof)

- Assume $n^2 = 2m$
- Need to show that $n = 2m'$ for some $m'$

Proof requires to find an appropriate integer $m'$. How can we give an expression for $m'$?

Second attempt (proof by Contraposition)

1. Assume $n$ is not even. Need to show that $n^2$ is not even.
**Theorem:** If $n^2$ is even, then $n$ is also even

First attempt (direct proof)

- Assume $n^2 = 2m$
- Need to show that $n = 2m'$ for some $m'$

Proof requires to find an appropriate integer $m'$. How can we give an expression for $m'$?

Second attempt (proof by Contraposition)

1. Assume $n$ is not even. Need to show that $n^2$ is not even.
2. Since $n$ is an integer, it must be odd, i.e., $n = 2m + 1$. 

**Theorem:** If $n^2$ is even, then $n$ is also even

First attempt (direct proof)

- Assume $n^2 = 2m$
- Need to show that $n = 2m'$ for some $m'$

Proof requires to find an appropriate integer $m'$. How can we give an expression for $m'$?

Second attempt (proof by Contraposition)

1. Assume $n$ is not even. Need to show that $n^2$ is not even.
2. Since $n$ is an integer, it must be odd, i.e., $n = 2m + 1$.
3. Therefore, $n^2 = (2m + 1)^2 = 4m^2 + 4m + 1 = 2(2m^2 + 2m) + 1$
Theorem: If \( n^2 \) is even, then \( n \) is also even.

First attempt (direct proof)

- Assume \( n^2 = 2m \)
- Need to show that \( n = 2m' \) for some \( m' \)

Proof requires to find an appropriate integer \( m' \). How can we give an expression for \( m' \)?

Second attempt (proof by Contraposition)

1. Assume \( n \) is not even. Need to show that \( n^2 \) is not even.
2. Since \( n \) is an integer, it must be odd, i.e., \( n = 2m + 1 \).
3. Therefore, \( n^2 = (2m + 1)^2 = 4m^2 + 4m + 1 = 2(2m^2 + 2m) + 1 \)
4. So, \( n^2 = 2m' + 1 \) is odd
Example (Proof by Contraposition)

**Theorem:** If $n^2$ is even, then $n$ is also even

First attempt (direct proof)

- Assume $n^2 = 2m$
- Need to show that $n = 2m'$ for some $m'$

Proof requires to find an appropriate integer $m'$. How can we give an expression for $m'$?

Second attempt (proof by Contraposition)

1. Assume $n$ is not even. Need to show that $n^2$ is not even.
2. Since $n$ is an integer, it must be odd, i.e., $n = 2m + 1$.
3. Therefore, $n^2 = (2m + 1)^2 = 4m^2 + 4m + 1 = 2(2m^2 + 2m) + 1$
4. So, $n^2 = 2m' + 1$ is odd
5. This proves that $n^2$ is not even.
Proof by Contradiction

This is a special case of proof by contraposition.

Remember: $True \rightarrow p$ is equivalent to $p$

Proving $True \rightarrow p$ by contraposition

- Assume $p$ is false
- Show that True is false: a contradiction!
Proof by Contradiction

This is a special case of proof by contraposition.

Remember:  \( \text{True} \rightarrow p \) is equivalent to \( p \)

Proving \( \text{True} \rightarrow p \) by contraposition

- Assume \( p \) is false
  - Show that \( \text{True} \) is false: a contradiction!

**Theorem:** \( p \) is true

**Proof:**

- Assume for contradiction that \( p \) is false
Proof by Contradiction

This is a special case of proof by contraposition.

Remember:  \( True \rightarrow p \) is equivalent to \( p \)

Proving \( True \rightarrow p \) by contraposition

- Assume \( p \) is false
- Show that True is false: a contradiction!

Theorem:  \( p \) is true

Proof:

- Assume for contradiction that \( p \) is false
- \( \ldots \) obtain a contradiction, i.e., proof something false
This is a special case of proof by contraposition.

Remember: $True \rightarrow p$ is equivalent to $p$

Proving $True \rightarrow p$ by contraposition

- Assume $p$ is false
- Show that $True$ is false: a contradiction!

**Theorem:** $p$ is true

**Proof:**

- Assume for contradiction that $p$ is false
- ... obtain a contradiction, i.e., proof something false
- Conclude that $p$ must be true.
**Theorem:** An integer $n$ cannot be both even and odd.
Theorem: An integer \( n \) cannot be both even and odd.

Fact: 1 is not even.

Proof:

1. Assume \( E(n) \) and \( O(n) \) for some integer \( n \)
2. By definition of \( E \), \( \exists m. n = 2m \)
3. By definition of \( O \), \( \exists m'. n = 2m' + 1 \)
4. Therefore, \( 2m = n = 2m' + 1 \).
5. Rearranging the terms, we get \( 1 = 2(m - m') \).
6. This proves that 1 is even, a contradiction!
Other common proof methods

Proof by cases: \((p \rightarrow q), (\neg p \rightarrow q) \implies q\)

- We want to prove \(q\).
Other common proof methods

Proof by cases: \((p \rightarrow q), (\neg p \rightarrow q) \implies q\)

- We want to prove \(q\).
- We consider two cases:
Other common proof methods

Proof by cases: \((p \rightarrow q), (\neg p \rightarrow q) \implies q\)

- We want to prove \(q\).
- We consider two cases:
  - First assume that \(p\) is true
Other common proof methods

Proof by cases: \((p \rightarrow q), (\neg p \rightarrow q) \implies q\)

- We want to prove \(q\).
- We consider two cases:
  - First assume that \(p\) is true
    - Show \(q\)
Other common proof methods

Proof by cases: $(p \rightarrow q), (\neg p \rightarrow q) \implies q$

- We want to prove $q$.
- We consider two cases:
  - First assume that $p$ is true
    - Show $q$
  - Next, assume that $p$ is false

Proofs of existence: show that $\exists x. p(x)$ is true
We show that $p(x)$ is true for $x = ???

Proofs by counterexample: show that $\forall x. p(x)$ is false
We show that $p(x)$ is false for $x = ???
Other common proof methods

Proof by cases: $(p \rightarrow q), (\neg p \rightarrow q) \implies q$

- We want to prove $q$.
- We consider two cases:
  - First assume that $p$ is true
    - Show $q$
  - Next, assume that $p$ is false
    - Show $q$. 
Other common proof methods

Proof by cases: \((p \rightarrow q), (\neg p \rightarrow q) \implies q\)

- We want to prove \(q\).
- We consider two cases:
  - First assume that \(p\) is true
    - Show \(q\)
  - Next, assume that \(p\) is false
    - Show \(q\).
- Since \(p\) is either true or false, and we showed that \(q\) is true in either case, we conclude that \(q\) is true.
Other common proof methods

Proof by cases: \((p \rightarrow q), (\neg p \rightarrow q) \implies q\)

- We want to prove \(q\).
- We consider two cases:
  - First assume that \(p\) is true
    - Show \(q\)
  - Next, assume that \(p\) is false
    - Show \(q\).
- Since \(p\) is either true or false, and we showed that \(q\) is true in either case, we conclude that \(q\) is true.
Other common proof methods

Proof by cases: \((p \rightarrow q), (\neg p \rightarrow q) \implies q\)

- We want to prove \(q\).
- We consider two cases:
  - First assume that \(p\) is true
    - Show \(q\)
  - Next, assume that \(p\) is false
    - Show \(q\).
- Since \(p\) is either true or false, and we showed that \(q\) is true in either case, we conclude that \(q\) is true.

Proofs of existence: show that \(\exists x. p(x)\) is true

- We show that \(p(x)\) is \textbf{true} for \(x = ???.\)
Proof by cases: \((p \rightarrow q), (\neg p \rightarrow q) \implies q\)

- We want to prove \(q\).
- We consider two cases:
  - First assume that \(p\) is true
    - Show \(q\)
  - Next, assume that \(p\) is false
    - Show \(q\).
- Since \(p\) is either true or false, and we showed that \(q\) is true in either case, we conclude that \(q\) is true.

Proofs of existence: show that \(\exists x. p(x)\) is true

- We show that \(p(x)\) is \textbf{true} for \(x = \text{???}\).

Proofs by counterexample: show that \(\forall x. p(x)\) is false

- We show that \(p(x)\) is \textbf{false} for \(x = \text{???}\).
Definition An integer $a$ divides an integer $b$ (written $a|b$), if there is an integer $c$ such that

(A) $a = b \cdot c$; (B) $a \cdot b = c$; (C) $b/a = c$; (D) $b = a \cdot c$;
**Definition** An integer $a$ *divides* an integer $b$ (written $a|b$), if there is an integer $c$ such that

(A) $a = b \cdot c$; (B) $a \cdot b = c$; (C) $b/a = c$; (D) $b = a \cdot c$;

Answer (D): $(a|b) \iff \exists c. b = a \cdot c$.

We also say that $b$ is a *multiple* of $a$. 
**Definition** Two integers $a, b$ are *congruent* modulo an integer $m$ (written $a \equiv_m b$) if $m$ divides $(a - b)$.

$$(a \equiv_m b) \iff m|(a - b) \iff \exists q. q \cdot m = a - b$$

**Theorem** (Division Theorem) For any integer $a$ and positive integer $b > 0$ there exists a (unique) pair of integers $(q, r)$ such that

- $a = qb + r$ and
- $0 \leq r < b$.

Vocabulary: $a$: dividend; $b$: divisor; $q$: quotient; $r$: reminder.
Uniqueness

A new quantifier: “There exists a unique $x$ such that $P(x)$”

- Think of $P$ as an equation.
- A solution to $P(x)$ is a value of $x$ such that $P(x)$ is true.
- What we are saying is that $P(x)$ has precisely one solution
- Sometimes this is denoted $\exists!x. P(x)$

Can we express $\exists!x. P(x)$ using the standard quantifiers?
A new quantifier: “There exists a unique $x$ such that $P(x)$”

- Think of $P$ as an equation.
- A solution to $P(x)$ is a value of $x$ such that $P(x)$ is true.
- What we are saying is that $P(x)$ has precisely one solution
- Sometimes this is denoted $\exists!x. P(x)$

Can we express $\exists!x. P(x)$ using the standard quantifiers?

- $\exists x. (P(x) \land U(x))$ where
  
- $U(x) = \text{“}P(x)\text{ has no other solution beside } x\text{”}$
  
- $U(x) = \forall y. (P(y) \rightarrow (x = y))$
- $\exists!x. P(x) \iff \exists x. (P(x) \land \forall y. (P(y) \rightarrow (x = y)))$. 
Let \((q, r)\) the result of the *division with remainder* of \(a\) by \(m\).

- The “uniqueness” part of the theorem tell us that \((q, r)\) are well defined.
- In may applications we are interested only in \(r\).
- Notation: \(r = a \mod m\). (\(a\%m\) in some programming languages.)

**Theorem:** For any integers \(a, b\) and positive integer \(m\) (modulus), \(a \equiv_m b\) if and only if \((a \mod m) = (b \mod m)\).

**Applications:** Hashing, modular arithmetics, cryptography.
Every integer is either even or odd, but not both.

**Theorem:** $\forall n. E(n) \oplus O(n)$.

- $E(n) \iff (n \mod 2 = 0)$
- $O(n) \iff (n \mod 2 = 1)$
- $0 \leq (n \mod 2) < 2$
- Equivalently, $(n \mod 2)$ equals either 0 or 1.
**Theorem:** For any integers $a, b, c$ and positive integer $m$, if $a \equiv_m b$ and $b \equiv_m c$, then $a \equiv_m c$.

**Proof:**

1. 
2. 
3. 
4. 
5. 
6.
**Theorem:** For any integers $a, b$ and positive integer $m$, if $m|a$ and $m|b$, then $m|(a + b)$.

**Proof:**

1. 
2. 
3. 
4. 
5. 
6. 