CSC165
Mathematical Expression and Reasoning for Computer Science

Module 8

Writing Proofs

Comments about Writing Proofs

- Avoid the notation "$\exists x = f(y) \in D: P(x, y)$"
  - Do not put things in between the variable and the domain
- For example, do not use "$\exists k = 2j^2 + 2j \in \mathbb{N}: n^2 = 2k + 1$"
- Instead you can write:

  Let $k_1 = 2j^2 + 2j$.
  Then $k_1 \in \mathbb{N}$.
  Then $n^2 = 2k_1 + 1$.

Comments about Writing Proofs

- Announce, in advance, when they are doing a proof by contrapositive or by contradiction
- For example you can write for an indirect proof:

  Let $x \in D$.

  \# proof by contraposition

  Assume $\neg Q(x)$.

  ....
- Also, you can write for a proof by contradiction:

  \# proof by contradiction

  Assume $\neg Q(x)$.

  ....

Comments about Writing Proofs

- Use “Let” to introduce a variable (both universal and existential)
  - Use one “Let” per variable
  - For example, for “$\forall x \in \mathbb{N}: [P(x) \rightarrow Q(x)]$”, you can write

  Let $x \in \mathbb{N}$.

   Assume $P(x)$.

    … .
- For example, for “$\exists x \in \mathbb{N}: [P(x) \wedge Q(x)]$”, you can write

  Let $x_0 = \cdots$.

  Then $x_0 \in \mathbb{N}$.

  … .

Comments about Writing Proofs

- Use “Assume” for:
  - The hypothesis of an implication
  - A case
  - The negation in a proof by contradiction
- For example, you can write:

  Assume $P(x)$.
  - Also:

  Case 2: Assume $x \geq 1$.
  - And:

  Assume there is a finite set of even integers.

Comments about Writing Proofs

- Always unpack an existential variable when using it. Rename the variable to something unique
- For example, for $\forall x \in \mathbb{N}: [(\exists y \in \mathbb{N}: [x = 2y]) \rightarrow (\exists y \in \mathbb{N}: [x^2 = 2y])]$:
  - You can write:

Let $x \in \mathbb{N}$.
  Assume $\exists y \in \mathbb{N}: [x = 2y]$.
    Let $y_0 \in \mathbb{N}$ such that $x = 2y_0$. # or Let $y_0 \in \mathbb{N}$ and assume $x = 2y_0$.
    Let $y_1 = 2y_0^2$.
    Then $y_1 \in \mathbb{N}$.
    Then $x^2 = (2y_0)^2 = 2(2y_0^2) = 2y_1$.
    Then $\exists y \in \mathbb{N}: x^2 = 2y$.
  Then $(\exists y \in \mathbb{N}: [x = 2y]) \rightarrow (\exists y \in \mathbb{N}: [x^2 = 2y])$.
Therefore, $\forall x \in \mathbb{N}: [(\exists y \in \mathbb{N}: [x = 2y]) \rightarrow (\exists y \in \mathbb{N}: [x^2 = 2y])]$.

Proof about Existential Statements

Direct Proof

- How to prove $\exists x \in \mathrm{D}: P(x)$
- Need one single example!
- Proof Structure:

Let $x_0 = \cdots$. # choose a particular element of the domain
Then $x_0 \in \mathrm{D}$. # this may be obvious, otherwise prove it
$\vdots$ # prove $P(x_0)$
Then $P(x_0)$. # x_0 satisfies P
Therefore, $\exists x \in \mathrm{D}: P(x)$. # introduce existential

Example

- Disprove $\forall x \in \mathbb{R}: [x^3 + 3x^2 - 4x \neq 12]$
- Negate then prove
- Prove $\exists x \in \mathbb{R}: [x^3 + 3x^2 - 4x = 12]$
- Thoughts:
  - We need to find a valid x… one example
  - For all reals: if $x^3 + 3x^2 - 4x = 12$, then $x^3 + 3x^2 = 4x + 12$
  - For all reals: if $x^3 + 3x^2 = 4x + 12$, then $x^2(x + 3) = 4(x + 3)$
  - Potential solutions: $x = -3, 2, -2$
  - Test potential solutions at $x^3 + 3x^2 - 4x = 12$
  - They work!

Proof

- Prove $\exists x \in \mathbb{R}: [x^3 + 3x^2 - 4x = 12]$
- Proof:

Let $x_0 = -2$. # choose a particular element of the domain

Then $x_0 \in \mathbb{R}$. # -2 is a real number

Then $x_0^3 + 3x_0^2 - 4x_0 = (-2)^3 + 3((-2)^2) - 4(-2)$ # plug $x_0 = -2$

$= -8 + 12 + 8$

$= 12.$ # -2 satisfies $P(x_0)$

Therefore, $\exists x \in \mathbb{R}: [x^3 + 3x^2 - 4x = 12]$. # introduce existential

Changing the Domain

- What happens if we change the domain?
- Prove $\exists x \in \mathbb{R}^+: [x^3 + 3x^2 - 4x = 12]$
- The valid example has to be from the positive reals
- $x = -3, -2$ cannot be used to prove this claim
- Proof:

Let $x_0 = 2$. # choose a particular element of the domain

Then $x_0 \in \mathbb{R}^+$. # 2 is a positive real number

Then ${x_0}^3 + 3x_0^2 - 4x_0 = (2)^3 + 3(2^2) - 4(2)$ # plug $x_0 = 2$

$= 8 + 12 - 8$

$= 12.$ # 2 satisfies $P(x_0)$

Therefore, $\exists x \in \mathbb{R}^+: [x^3 + 3x^2 - 4x = 12]$. # introduce existential

Direct Proof of Universally Quantified Implications

Proof of a UQI

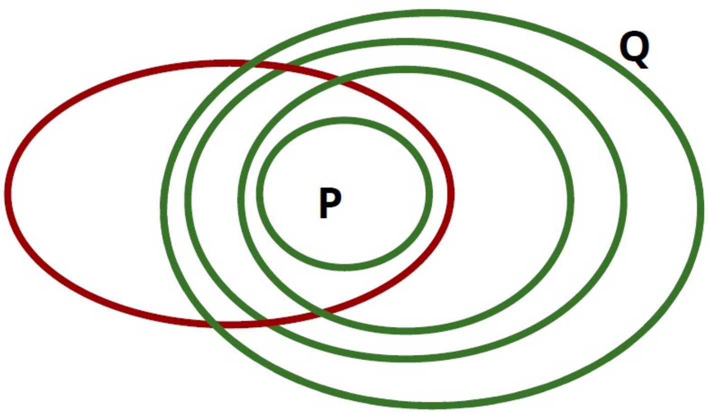
- Find a proof for $\forall x \in D: P(x) \rightarrow Q(x)$
- That means, prove that $[\forall x \in D: P(x) \rightarrow Q(x)]$ is true
- $P(x)$ and $Q(x)$ are predicates; i.e., Boolean functions
- The "proof process" means:
  - Proving for all members x of domain D, if x has the property P, then x has the property Q
  - Whenever x makes $P(x)$ true, then x makes $Q(x)$ true
  - In Venn diagram, we want to show that P is completely contained in Q
  - We do not intend to prove that $P(x)$ is true for all x in domain D

Thinking Process

- Goal: find a proof for $\forall x \in D: P(x) \rightarrow Q(x)$
- Key to solution is finding the "chain" between $P(x)$ and $Q(x)$
  - $\forall x \in D: P(x) \rightarrow R_1(x)$
  - $\forall x \in D: R_1(x) \rightarrow R_2(x)$
  - ….
  - $\forall x \in D: R_{n-1}(x) \rightarrow R_n(x)$
  - $\forall x \in D: R_n(x) \rightarrow Q(x)$
  - Therefore, $\forall x \in D: P(x) \rightarrow Q(x)$

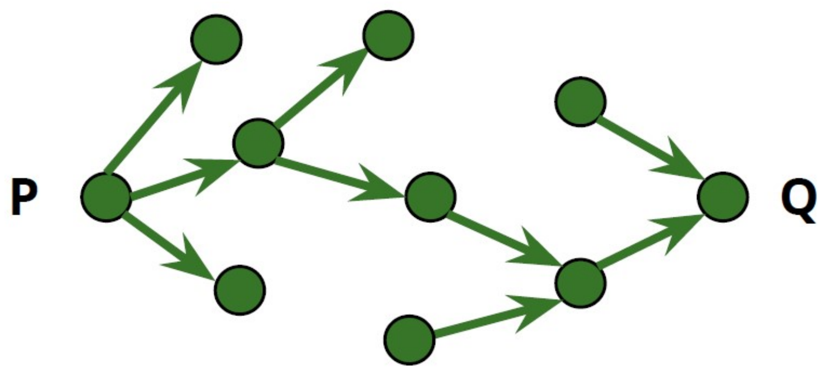
The "Chain"

- $\forall x \in D: P(x) \rightarrow R_1(x) \rightarrow R_2(x) \rightarrow \cdots \rightarrow R_{n-1}(x) \rightarrow R_n(x) \rightarrow Q(x)$



The “Chain”

- $\forall x \in D: P(x) \rightarrow R_1(x) \rightarrow R_2(x) \rightarrow \cdots \rightarrow R_{n-1}(x) \rightarrow R_n(x) \rightarrow Q(x)$



Writing the Proof: $\forall x \in D: P(x) \rightarrow Q(x)$

Let $x \in D$.	# assume an arbitrary member of the domain
Assume $P(x)$.	# assume $P(x)$ to be true
Then $R_1(x)$.	# if $P(x)$ is true, then $R_1(x)$ is true
Then $R_2(x)$.	# if $R_1(x)$ is true, then $R_2(x)$ is true
…	
Then $R_n(x)$.	# if $R_{n-1}(x)$ is true, then $R_n(x)$ is true
Then $Q(x)$.	# if $R_n(x)$ is true, then $Q(x)$ is true
Then $P(x) \rightarrow Q(x)$.	# if $P(x)$ is true, then $Q(x)$ is true
Therefore, $\forall x \in D: P(x) \rightarrow Q(x)$.	# since x is an arbitrary member of the domain, then (if $P(x)$ is true, then $Q(x)$ is true) is true for all members of D

Proof Example

- Prove $\forall n \in \mathbb{N}$: n is odd, then n^2 is odd
- What do we have?
  - $\mathbb{N}$: set of natural numbers $\{0,1,2,\dots\}$
  - n is a dummy variable, it could have been x or y
  - We want to prove that [$\forall n \in \mathbb{N}$: n is odd, then n^2 is odd] is a true statement
  - We want to prove that for all members n of natural numbers, if n has the property of being odd, then square of n has the property of being odd
  - Whenever n is odd, square of n is odd
  - We do not intend to prove that if n is not odd, then n^2 is something

Proof Example

- Since 1 is odd, the statement claims that 1^2 is odd
- Since 3 is odd, the statement claims that 3^2 is odd
- Since 2 is not odd, the statement does not directly claim that 2^2 is odd
- Since 4 is not odd, the statement does not directly claim that 4^2 is odd

n	n is odd?	n^2	n^2 is odd	
1	True	1	True	Okay
3	True	9	True	Okay
0	False	0	False	Irrelevant
2	False	4	False	Irrelevant

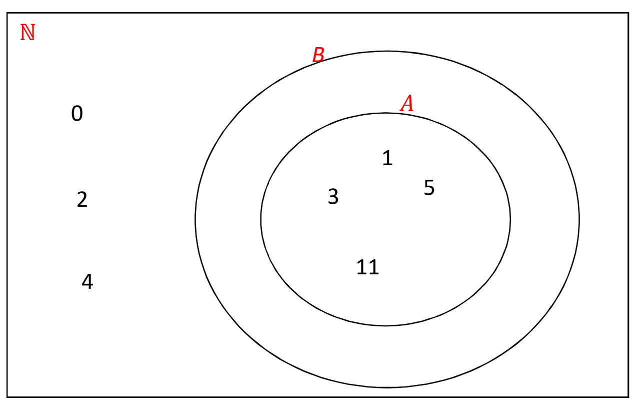
Proof Example

- Consider two sets of numbers:
  - A: The set of all natural numbers that are odd
  - B: The set of all natural numbers that when squared are odd
- Look at these sets on a number line:

```
A:              ●       ●       ●       ●...
B:              ●       ●       ●       ●...
     <----------|-----|------|-----|-----|-----|-----|-----|------->
                0     1      2     3     4     5     6     7
```


Proof Example

- Venn Diagram
- A is fully contained in B



Proof Process

- n is odd: $\exists j \in \mathbb{N}: n = 2(j) + 1$
- j is a dummy variable

- n^2 is odd: $\exists k \in \mathbb{N}: n^2 = 2(k) + 1$
- k is also a dummy variable

Odd number	
1	0(2)+1
3	1(2)+1
5	2(2)+1
…	…
n	$\exists j \in \mathbb{N}: n = 2(j) + 1$

Thinking Process

- n is odd:
- Then $\exists j \in \mathbb{N}: n = 2j + 1$.
- Then $n^2 = n.n$
  $= (2j + 1).(2j + 1)$
  $= 4j^2 + 4j + 1$
  $= 2(2j^2 + 2j) + 1$.
- Let $k = 2j^2 + 2j$.
- Then $n^2 = 2k + 1$
- If $j \in \mathbb{N}$, then $k \in \mathbb{N}$.
- Then, $\exists k \in \mathbb{N}: n^2 = 2k + 1$.
- Then n^2 is odd.

Writing the Proof: $\forall n \in \mathbb{N}: n$ is odd $\rightarrow n^2$ is odd

Let $n \in \mathbb{N}$. # n is generic natural number
Assume n is odd. # assume P is true
Then $\exists j \in \mathbb{N}: n = 2j + 1$. # definition of odd number
Let $j_0 \in \mathbb{N}$ such that $n = 2j_0 + 1$.
Then $n^2 = (2j_0 + 1).(2j_0 + 1) = 2(2j_0^2 + 2j_0) + 1$.
Let $k_0 = 2j_0^2 + 2j_0$.
Then $k_0 \in \mathbb{N}$.
Then $n^2 = 2k_0 + 1$.
Then $\exists k \in \mathbb{N}: n^2 = 2k + 1$. #
Then n^2 is odd. # prove that Q is true
Then n is odd $\rightarrow n^2$ is odd. # $P \rightarrow Q$ is true for a generic n
Therefore, $\forall n \in \mathbb{N}: n$ is odd $\rightarrow n^2$ is odd. # $P \rightarrow Q$ is true for all $n \in \mathbb{N}$

Direct Proof Example

Proof Example

- Prove $\forall n \in \mathbb{N}$: if n is even, then n^2 is even
- We want to prove that [$\forall n \in \mathbb{N}$: n is even, then n^2 is even] is a true statement
- For all members n of natural numbers, if n has the property of being even, then square of n has the property of being even
- Whenever n is even, square of n is even
- For later, think about proving the converse

Proof Example

- Since 1 is odd, the statement does not directly claim that 1^2 is even
- Since 3 is odd, the statement does not directly claim that 3^2 is even
- Since 0 is even, the statement claims that 0^2 is even
- Since 2 is even, the statement claims that 2^2 is even
- Since 4 is even, the statement claims that 4^2 is even

n	n is even?	n^2	n^2 is even	
1	False	1	False	Irrelevant
3	False	9	False	Irrelevant
0	True	0	True	Okay
2	True	4	True	Okay

Proof Example

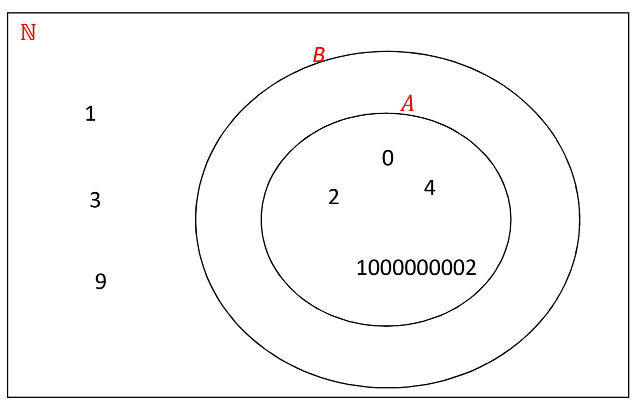
- Consider two sets of numbers:
  - A: The set of all natural numbers that are even
  - B: The set of all natural numbers that when squared are even
- Look at these sets on a number line:

```
A:        ●         ●         ●         ●…
B:        ●         ●         ●         ●…
<----------|-----|------|-----|-----|-----|-----|-----|------->
           0     1      2     3     4     5     6     7
```


Proof Example

- A is fully contained in B
- n is even: $\exists j \in \mathbb{N}: n = 2(j)$
- n^2 is even: $\exists k \in \mathbb{N}: n^2 = 2(k)$

Even number	
0	0(2)
2	1(2)
4	2(2)
…	…
n	$\exists j \in \mathbb{N}: n = 2(j)$



Proof: $\forall n \in \mathbb{N}$: if n is even, then n^2 is even

Let $n \in \mathbb{N}$. # n is generic natural number

Assume n is even. # assume P is true

Then $\exists j \in \mathbb{N}: n = 2j$. # definition of even number

Let $j_0 \in \mathbb{N}$ such that $n = 2j_0$.

Then $n^2 = (2j_0).(2j_0) = 2(2j_0^2)$.

Let $k_0 = 2j_0^2$.

Then $k_0 \in \mathbb{N}$.

Then $n^2 = 2k_0$.

Then $\exists k \in \mathbb{N}: n^2 = 2k$. # definition of even number

Then n^2 is even. # prove that Q is true

Then n is even $\rightarrow n^2$ is even. # $P \rightarrow Q$ is true for a generic n

Therefore, $\forall n \in \mathbb{N}: n$ is even $\rightarrow n^2$ is even. # $P \rightarrow Q$ is true for all $n \in \mathbb{N}$

Practice Problem

- Prove $\forall n \in \mathbb{N}$: if n is a multiple of 4, then n^2 is a multiple of 4

- What is the converse?
- Is it true or false?
- Can you prove/disprove the converse?

Proof by Contraposition

Contrapositive

- The contrapositive of $\forall x \in D: P(x) \rightarrow Q(x)$ is $\forall x \in D: \neg Q(x) \rightarrow \neg P(x)$
- Instead of "directly" proving $\forall x \in D: P(x) \rightarrow Q(x)$, we can equivalently prove $\forall x \in D: \neg Q(x) \rightarrow \neg P(x)$
- Proof by Contraposition is sometimes called "indirect proof"
- Chain of implication: $\neg Q(x) \rightarrow C_1(x) \rightarrow \cdots \rightarrow C_n(x) \rightarrow \neg P(x)$
- When is this useful?
  - When the reverse direction is easier to prove than the original

Indirect Proof Structure

- Prove $\forall x \in D: P(x) \rightarrow Q(x)$
- Generic proof:

Let $x \in D$. # x is a typical element of domain D
  # proof by contraposition
  Assume $\neg Q(x)$. # negation of the consequent!
    Then $C_1(x)$. # find the chain
    ⋮
    Then $C_n(x)$. # find the chain
    Then $\neg P(x)$. # negation of the antecedent!
  Then $\neg Q(x) \rightarrow \neg P(x)$. # assuming $\neg Q(x)$ leads to $\neg P(x)$
  Then $P(x) \rightarrow Q(x)$. # implication is equivalent to contrapositive
Therefore, $\forall x \in D: P(x) \rightarrow Q(x)$. # introduce universal quantifier

Example

- Prove $\forall n \in \mathbb{N}$: if n^2 is even, then n is even
- Contrapositive: $\forall n \in \mathbb{N}$: n is not even, then n^2 is not even
- For natural numbers:
  - Not odd: even number
  - Not even: odd number
- Contrapositive: $\forall n \in \mathbb{N}$: if n is odd, then n^2 is odd
- To indirectly prove that $\forall n \in \mathbb{N}$: if n^2 is even, then n is even we can directly prove its contrapositive $\forall n \in \mathbb{N}$: if n is odd, then n^2 is odd

Proof: $\forall n \in \mathbb{N}$: n^2 is even $\rightarrow$ n is even

Let $n \in \mathbb{N}$. # x is a typical element of domain D
 # proof by contraposition
 Assume n is odd. # assume $\neg Q$ is true
  Then $\exists j \in \mathbb{N}: n = 2j + 1$. # definition of odd number
  Let $j_0 \in \mathbb{N}$ such that $n = 2j_0 + 1$.
  Then $n^2 = (2j_0 + 1).(2j_0 + 1) = 2(2j_0^2 + 2j_0) + 1$.
  Let $k_0 = 2j_0^2 + 2j_0$.
  Then $k_0 \in \mathbb{N}$.
  Then $n^2 = 2k_0 + 1$.
  Then $\exists k \in \mathbb{N}: n^2 = 2k + 1$. # def. of odd number
  Then n^2 is odd. # prove that $\neg P$ is true
 Then n is odd $\rightarrow n^2$ is odd. # $\neg Q \rightarrow \neg P$ is true for a generic n
 Then n^2 is even $\rightarrow n$ is even. # implication is equivalent to contrapositive
Therefore, $\forall n \in \mathbb{N}$: n^2 is even $\rightarrow n$ is even. # introduce universal quantifier

Example

- Prove $\forall n \in \mathbb{N}$: if n^2 is odd, then n is odd
- Contrapositive: $\forall n \in \mathbb{N}$: n is not odd, then n^2 is not odd
- For natural numbers:
  - Not odd: even number
  - Not even: odd number
- Contrapositive: $\forall n \in \mathbb{N}$: if n is even, then n^2 is even
- To indirectly prove that $\forall n \in \mathbb{N}$: if n^2 is odd, then n is odd we can directly prove its contrapositive $\forall n \in \mathbb{N}$: if n is even, then n^2 is even

Proof: $\forall n \in \mathbb{N}$: n^2 is odd $\rightarrow n$ is odd

Let $n \in \mathbb{N}$. # x is a typical element of domain D
proof by contraposition
Assume n is even. # assume P is true
Then $\exists j \in \mathbb{N}: n = 2j$. # definition of even number
Let $j_0 \in \mathbb{N}$ such that $n = 2j_0$.
Then $n^2 = (2j_0).(2j_0) = 2(2j_0^2)$.
Let $k_0 = 2j_0^2$.
Then $k_0 \in \mathbb{N}$.
Then $n^2 = 2k_0$.
Then $\exists k \in \mathbb{N}: n^2 = 2k$. # definition of even number
Then n^2 is even. # prove that Q is true
Then n is even $\rightarrow n^2$ is even. # $P \rightarrow Q$ is true for a generic n
Then n^2 is odd $\rightarrow n$ is odd. # implication is equivalent to contrapositive
Therefore, $\forall n \in \mathbb{N}$: n^2 is odd $\rightarrow n$ is odd. # introduce universal quantifier