More Proofs

CSCI 170 Spring 2021

Sandra Batista

1.1-1.2

Proofs

- **Constructive Proof**
- Non-constructive Proof
- Proof by Cases
- Direct Proof of Implication
- Proof by Contraposition
- Proof by Contradiction
- Disprove a statement

1.1-1.2

Proof Method: Constructive Proof

A **constructive proof** is one that proves that a solution or property exists by giving the solution or instance of the property directly.

Claim: Every 8x8 checkerboard can be tiled by dominos, 2x1 rectangular tiles with a 1 dot in the first square and 2 dots in the second. The tiles of the domino are the same size as each square of the checkerboard.

What is this statement in predicate logic? What is its negation?

let B be 8×8 checkerboards.

$P(x)$: x can be tiled with dominos

$$\forall b \in B \; P(b)$$

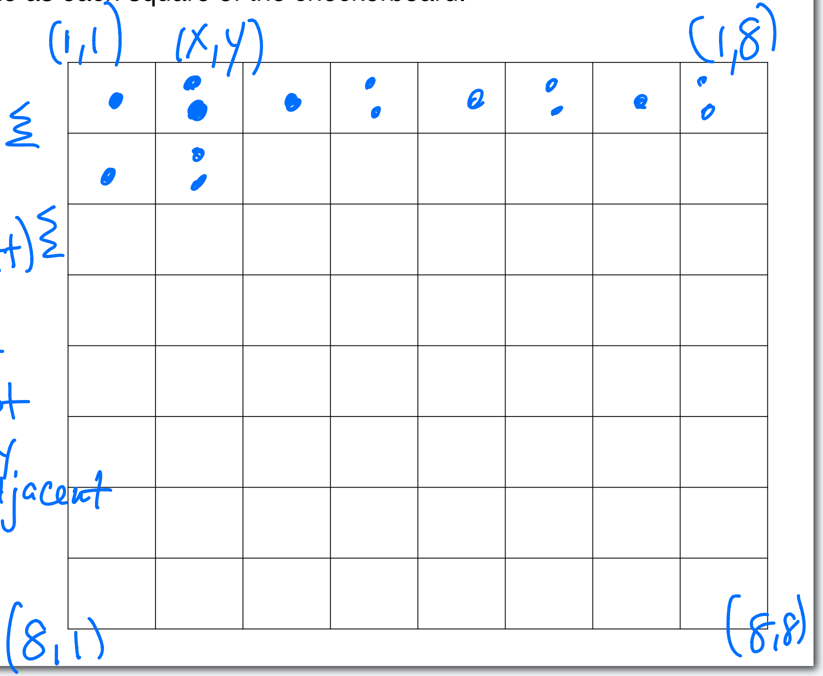
$$\exists b \in B \; \neg P(b)$$

Constructive Proof Example 1

Claim: Every 8x8 checkerboard can be tiled by dominos, 2x1 rectangular tiles with a 1 dot in the first square and 2 dots in the second. The tiles of the domino are the same size as each square of the checkerboard.

Proof: Give an algorithm to tile the checkerboard.

```
for(int x=1; x≤8; x++){
  for (int y=1; y≤8; y++){
    if (y%2==1) //odd
    {place domino w/ 1 dot square on column y
     and 2 dot on adjacent tile
    }
    y++;
  }
}
```



Proofs

- Constructive Proof
- **Non-constructive Proof**
- Proof by Cases
- Direct Proof of Implication
- Proof by Contraposition
- Proof by Contradiction
- Disprove a statement

1.1–1.2

Proof Method: Non-constructive Proof

A **non-constructive proof** is when a proof shows that a solution exists without giving the solution directly.

Claim: At a dinner with 9 guests at least 2 must have been born on the same day of the week.

Proof: PHP

Let A be set of guests $|A| = 9$

Let B be the days of week $|B| = 7$

$f: A \to B$ $f(a) =$ day of week on which born

Since $|A| > |B|$, there exist at least 2 guests born on same day of the week (by PHP).

Proof Method: Proof by Cases

A **proof by cases** is when a proof of a claim exhaustively considers all cases that are possible for the claim and shows that the claim would still hold under all such cases.

Cases are often mutually exclusive.

Claim: There exists irrational numbers x and y such that x^y is rational.
Proof by cases:
Let $x = y = \sqrt{2}$

Case 1: If $\sqrt{2}^{\sqrt{2}}$ is rational, then done!

Case 2: If $\sqrt{2}^{\sqrt{2}}$ is not rational, then let

$$x' = \sqrt{2}^{\sqrt{2}} \quad y' = \sqrt{2}$$

$$(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = 2$$

Proofs

- Constructive Proof
- Non-constructive Proof
- Proof by Cases
- **Direct Proof of Implication**
- Proof by Contraposition
- Proof by Contradiction
- Disprove a statement

1.1–1.2

Useful Refresher

1. If an integer n is **odd**, then there exists an integer k such that **n = 2k +1**. If an integer n is **even**, then there exists an integer k such that **n = 2k**.

2. If n is a **rational**, then there exists integers p and q that share no prime factors and q is non-zero such that **n = p/q**.

3. An integer d evenly **divides** an integer n if it is a factor. Similarly the remainder when we divide n by d is 0. We also say that n is divisible by d.

   $n = dk$ for some integer k

4. If n = mk + r and we divide n by m, we will be left with a remainder of r: **n mod m = r**

5. All even numbers are 0 mod 2. All odd numbers are 1 mod 2. Whether an integer is even or odd is referred to as its **parity**.

Proof Method: Direct Proof of an Implication

In a **direct proof** of implication we assume the premise P and use logic and rules of inference to show that the conclusion Q follows.

Exercise: If r and s are rational, then r+s is rational.

Proof: If r is rational $\exists\, p_1, q_1 \in \mathbb{Z}$ $q_1 \neq 0$ $r = \frac{p_1}{q_1}$,

and s is rational $\exists\, p_2, q_2 \in \mathbb{Z}$ $q_2 \neq 0$ $s = \frac{p_2}{q_2}$

$\Rightarrow r + s = \frac{p_1 q_2 + p_2 q_1}{q_1 q_2} = \frac{p_1}{q_1} + \frac{p_2}{q_2}$

Proof Method: Direct Proof of an Implication

In a **direct proof** of implication we assume the premise P and use logic and rules of inference to show that the conclusion Q follows.

Exercise: If r and s are rational, then r+s is rational.

Proof (continued): $\Rightarrow q_1 \neq q_2 \neq 0 \Rightarrow q_1 q_2 \neq 0$

$q_1 q_2 \in \mathbb{Z}$ $\Rightarrow p_1 q_2 \in \mathbb{Z},\ p_2 q_1 \in \mathbb{Z}$

$\Rightarrow p_1 q_2 + p_2 q_1 \in \mathbb{Z}$

Proofs

- Constructive Proof
- Non-constructive Proof
- Proof by Cases
- Direct Proof of Implication
- **Proof by Contraposition**
- Proof by Contradiction
- Disprove a statement

1.1–1.2

Proof Method: Proof by Contraposition

The contrapositive of P implies Q is not Q implies not P.

In a **proof by contraposition** of an implication P implies Q, we assume the negation of the conclusion, i.e. not Q, and use logic and rules of inference to show that the negation of the premise, i.e. not P, follows.

State the contrapositive and prove it directly.

Exercise: Let n be an integer. If 3n+2 is odd, then n is odd.

Proof by contraposition:
State the contrapositive and prove it directly.

If n even $\Rightarrow 3n+2$ is even

Proof Method: Proof by Contraposition

The contrapositive of P implies Q is not Q implies not P.

In a **proof by contraposition** of an implication P implies Q, we assume the negation of the conclusion, i.e. not Q, and use logic and rules of inference to show that the negation of the premise, i.e. not P, follows.

State the contrapositive and prove it directly.

Exercise: Let n be an integer. If 3n+2 is odd, then n is odd.
Proof by contraposition:

Assume n is even $\Rightarrow \exists k \in \mathbb{Z}$ $n = 2k$

$\Rightarrow 3n + 2 = 3(2k) + 2 = 2(3k+1)$

Since $3k+1 \in \mathbb{Z} \Rightarrow 3n+2$ is even

Proofs

- Constructive Proof
- Non-constructive Proof
- Proof by Cases
- Direct Proof of Implication
- Proof by Contraposition
- **Proof by Contradiction**
- Disprove a statement

1.1–1.2

Proof Method: Proof by Contradiction

To prove a statement by **contradiction**: Negate the statement and show any contradiction.

Template for an implication: P implies Q

1)This implication is logically equivalent to not P or Q

$$p \rightarrow q \equiv \neg p \vee q$$

2)Assume the negation:

$$\neg(\neg p \vee q) \equiv p \wedge \neg q$$

3)Show any contradiction. When we show a contradiction occurs, we show that the **negation is false, so the original statement is true.**

Proof by Contradiction Example 1

Contrapositive: If n is even $\Rightarrow$ 3n+2 is even.

Exercise: Let n be an integer. If 3n+2 is odd, then n is odd.

Proof by contradiction: Negation: 3n + 2 is odd and n is even.

Assume 3n + 2 is odd and n is even.

Let $n = 2k$ for some $k \in \mathbb{Z}$ (since n is even)

$$3n+2 = 3(2k)+2 = 2(3k+1)$$

Since $3k+1 \in \mathbb{Z}$ $\Rightarrow$ 3n+2 even $\boxed{\Rightarrow\Leftarrow}$

This is a $\boxed{\text{contradiction}}$ because we assumed 3n+2 is odd.

Proof by Contradiction Example 2

Exercise: Show square root of 12 is irrational.

Proof by contradiction: Assume negation: $\sqrt{12}$ is rational. $\sqrt{12} = \frac{p}{q}$ where $p, q \in \mathbb{Z}$ sharing no prime factors $q \neq 0$.

$$\Rightarrow 12 = \frac{p^2}{q^2} \Rightarrow 2^2 3 q^2 = p^2$$

i) 2 divides p : $2(2\,3q^2) = p^2$

ii) 3 divides p : $3(2^2 q^2) = p^2$

$\Rightarrow$ i) $p = 2c_1$ for some $c_1 \in \mathbb{Z}$

ii) $p = 3c_2$ for some $c_2 \in \mathbb{Z}$

Proof by Contradiction Example 2

Exercise: Show square root of 12 is irrational.

Proof by contradiction (continued):

i) $p = 2c_1, c_1 \in \mathbb{Z}$ $\Rightarrow$ 3 divides c_1

$2^2 3 q^2 = (2c_1)^2$ $\Rightarrow$ 3 divides p ✓

$3q^2 = c_1^2$

ii) $p = 3c_2$, $c_2 \in \mathbb{Z}$

$2^2 3 q^2 = (3c_2)^2$

$2^2 q^2 = 3c_2^2$

Since 3 does not divide 2 $\Rightarrow$ 3 divides q ✓

$\Rightarrow \Leftarrow$ p, q share no prime factors $(q \neq 0)$

Proofs

1.1–1.2

- Constructive Proof
- Non-constructive Proof
- Proof by Cases
- Direct Proof of Implication
- Proof by Contraposition
- Proof by Contradiction
- Disprove a statement