FA23

EECS 203 Discussion 3

Proofs, Introduction to Proof Techniques

Admin Notes:

Forms:

- Two beginning of semester surveys on Canvas.
  - **Due:** Thursday, Sept. 14th @11:59 pm
- Exam Date Confirmation Survey
  - **Due:** Tuesday, Sept. 19th @11:59 pm
  - Fill this out even if you don't have an exam conflict!
- They are each worth a few points so fill them out!

Homework:

- Homework/Groupwork 2 was due Sept. 14th
- Homework/Groupwork 3 should be released! It will be due **Sept. 21st**
  - **Don't forget to match pages!**
  - Please note as soon as you press submit you've successfully submitted by the deadline, you can still match the pages with no rush, that doesn't add to your submission time.
- Groupwork:
  - It can be done alone, but the problems tend to be more difficult, and the goal is for you to puzzle them out with others!
  - Discussion section is a great place to find a group!
  - There is also a pinned Piazza thread for searching for homework groups.

Proof Techniques

Making a Valid Argument (Writing a Proof)

- **Argument/Proof:** An **argument** for a statement S is a sequence of statements ending with S. S is called the **conclusion**. An argument starts with some beginning statements you assume are true, called the **premises**.

- **Valid Argument/Proof:** An argument is **valid** if every statement after the premises is implied (→) by the some combination of the statements before it.
    - Whenever the premises are true, the conclusion must be true.

- Today we will be discussing word-style proofs

Intro To Word-Style Proofs
(Direct Proof)

Useful Definitions

*Note: **iff** stands for if and only if (↔)

- **Even:** An integer **x** is even iff there exists an integer k such that $x = 2k$
- **Odd:** An integer **x** is odd iff there exists an integer k such that $x = 2k + 1$
- **Rational:** A number **x** is rational iff it can be written as the quotient of two integers. $x = p/q$
- **Irrational:** Not rational–cannot be written as the quotient of two integers
- **Prime:** A prime number **p** is a number greater than 1 whose only factors are 1 and itself. $\forall x\ [x|p \rightarrow (x=1 \lor x=p)]$
- **Composite:** A whole number **p** is composite if it has at least one divisor other than 1 and itself. $\exists x\ [x\neq1 \land x\neq p \land x|p]$

Proof Methods

- **Direct Proof:** Proves $p \rightarrow q$ by showing

  $p \rightarrow \text{stuff} \rightarrow q$

- **Proof by Contraposition:** Proves $p \rightarrow q$ by showing

  $\neg q \rightarrow \text{stuff} \rightarrow \neg p$

- **Proof by Contradiction:** next week

- **Proof by Cases:** next week

Some Methods of Proving $p \rightarrow q$

- **Direct Proof:**
  Proves $p \rightarrow q$ by showing **$p \rightarrow$ stuff $\rightarrow q$**
- **Proof by Contraposition:**
  Proves $p \rightarrow q$ by showing **$\neg q \rightarrow$ stuff $\rightarrow \neg p$**
  (Once you show $\neg q \rightarrow \neg p$, you can immediately conclude $p \rightarrow q$ by contraposition)
- **Proof by Contradiction:**
  Assume p and $\neg q$ are true. Derive a contradiction (F), by arriving at a mathematically incorrect statement (ex: $0 = 2$) or two statements that contradict each other ($x = y$ and $x \neq y$). Therefore, $p \rightarrow q$.
  $(p \land \neg q) \rightarrow F \rightarrow \neg(p \land \neg q) \equiv \neg p \lor q \equiv p \rightarrow q$
- **Proof by Cases:**
  Break p into cases and show that each case implies q (in which case $p \rightarrow q$).
  $p \rightarrow p_1 \lor p_2 \lor \ldots \lor p_n \rightarrow q$

Proving “For All” and “There Exists” Statements

<u>Claim:</u> For all x, P(x).

<u>Proof Template:</u>

Let x be an **arbitrary** domain element

…

Thus, P(x).

Therefore, P(x) holds for all x in the domain.

<u>Claim:</u> There exists an x such that P(x).

<u>Proof Template:</u>

Consider x = __ [specific domain element]

… show that P(x) holds for that value of x.

Note: Assuming an arbitrary domain element “without loss of generality” (WLOG) can simplify proofs.

Notes:

- **Even:** An integer x is even iff there exists an integer k such that **$x = 2k$**
- **Odd:** An integer x is odd iff there exists an integer k such that **$x = 2k + 1$**

Problem:

1. Odd Proof

Prove or disprove: The sum of an even and an odd integer is always odd.

Solution:

1. Odd Proof

Prove or disprove: The sum of an even and an odd integer is always odd.

Solution: We will prove this statement.
Without loss of generality (WLOG), let x be an **arbitrary** even integer and y be an **arbitrary** odd integer. By definition, then, x and y can be written as $x = 2n$ and $y = 2m + 1$ for some integers n and m. Looking at their sum, we have

$$\begin{aligned} x + y &= 2n + 2m + 1 \\ &= 2(n + m) + 1. \end{aligned}$$

Since $x + y = 2c + 1$, where c is the integer $n + m$, then by definition, $x + y$ is odd. Therefore, this relation holds for all even x and odd y, and we have proved that the sum of an even and an odd integer is odd.

Notes:

- **Even:** An integer x is even iff there exists an integer k such that **x = 2k**
- **Odd:** An integer x is odd iff there exists an integer k such that **x = 2k + 1**

Problem:

2. Even Proof

Prove (using a direct proof) that if $m + n$ and $n + p$ are even integers, where m, n, and p are integers, then $m + p$ is even.

Solution:

2. Even Proof

Prove (using a direct proof) that if $m + n$ and $n + p$ are even integers, where m, n, and p are integers, then $m + p$ is even.

Solution: Using a Direct Proof,

- Let $m + n$ and $n + p$ be **arbitrary** even integers, $m + n = 2a$ and $n + p = 2b$, for some (arbitrary) integers a and b.
- $m + p = (m + n) + (n + p) - 2n = 2a + 2b - 2n = 2(a + b - n)$
- Since $a + b - n$ is an integer, let it be k.
- Hence, $m + p = 2k =$ even integer

Therefore, the statement "if $m + n$ and $n + p$ are even integers, where m, n, and p are integers, then $m + p$ is even" holds for all even $m + n$ and $n + p$.

Disproof

To **disprove** a statement means to **prove the negation** of that statement:

Disprove $P(x) \equiv$ Prove $\neg P(x)$

Note that if the statement you are trying to disprove is a for-all statement, all you need to disprove it is a singular counter example since $\neg \forall x P(x) \equiv \exists x \neg P(x)$.

Example: Disprove it's raining today ≡ **Prove** it's not raining today 🌞

Example: Disprove $P \rightarrow Q \equiv$ **Prove** $\neg(P \rightarrow Q) \equiv \neg(\neg P \vee Q) \equiv (P \wedge \neg Q)$

Problem:

3. Disproofs; Two Sides of the Same Coin

a. **Disprove:** For all real numbers x and y, if they sum to zero, one of them is negative and the other is positive.

b. **Disprove:** For all nonzero rational numbers x and y, if they are multiplicative inverses, $x \neq y$.
Note: Two numbers are multiplicative inverses if their product is 1.

Solution:

3. Disproofs; Two Sides of the Same Coin

a. **Disprove:** For all real numbers x and y, if they sum to zero, one of them is negative and the other is positive.

b. **Disprove:** For all nonzero rational numbers x and y, if they are multiplicative inverses, $x \neq y$.
Note: Two numbers are multiplicative inverses if their product is 1.

Solution: With for all disproofs, we need to find a counterexample (some values of x and y that make this statement false).

a. Consider $x = 0$ and $y = 0$.
$x + y = 0$, and since 0 is neither negative nor positive, this if-then statement false.

Therefore, it is not true for all real numbers x and y, that if they sum to zero, one of them is negative and the other is positive.

b. Consider $x = 1$ and $y = 1$.
$x \cdot y = 1$, and $x = y$, so this if-then statement is false.

Therefore, it is not true for all nonzero rational numbers x and y that if they are multiplicative inverses, $x \neq y$.

Problem:

4. Quantifier Proofs

For each part, translate the statement into logical connectives and math symbols. Then prove or disprove it.

a. Each non-zero rational number has a multiplicative inverse (also a rational number) such that their product is 1.

b. Each integer has a multiplicative inverse that is also an integer.
Note: Two numbers are multiplicative inverses if their product is 1.

Solution:

4. Quantifier Proofs

For each part, translate the statement into logical connectives and math symbols. Then prove or disprove it.

a. Each non-zero rational number has a multiplicative inverse (also a rational number) such that their product is 1.

b. Each integer has a multiplicative inverse that is also an integer.
Note: Two numbers are multiplicative inverses if their product is 1.

Solution:

a. Let x and y come from the domain of all non-zero rational numbers.

$$\forall x \exists y [xy = 1]$$

Prove:

- Take an arbitrary non-zero rational number x.
- By definition of rational numbers, $x = \dfrac{p}{q}$ for some integers p and q where $q \neq 0$.
- Since $x \neq 0$, $p \neq 0$.
- Let $y = \dfrac{q}{p}$. (We can do this since $p \neq 0$)
- y is a rational number by definition
- Since $q \neq 0$, $y \neq 0$.
- $xy = \dfrac{p}{q} \cdot \dfrac{q}{p} = 1$

Thus, for all non-zero rational numbers x there exists an inverse rational number y such that $xy = 1$.

b. Let x and y come from the domain of non-zero integers.

$$\forall x \exists y [xy = 1]$$

Disprove:
Consider $x = 2$ (an element of the nonzero integers). Its (only) multiplicative inverse is $\frac{1}{2}$, but $\frac{1}{2}$ is not an integer. Thus, this for all statement is false (since to be true it would need to be true for every nonzero integer).

Proof by Contraposition

Recall: Proof Methods

- **Proof by Contraposition:** Proves $p \rightarrow q$ by showing
  $\neg q \rightarrow$ stuff $\rightarrow \neg p$
- Works because **$p \rightarrow q \equiv \neg q \rightarrow \neg p$**

p	q	$p \rightarrow q$	$\neg q$	$\neg p$	$\neg q \rightarrow \neg p$
T	T	T	F	F	T
T	F	F	T	F	F
F	T	T	F	T	T
F	F	T	T	T	T

Problem:

5. Proof by Contrapositive I

Prove for all real numbers that if $n^2 + 2$ is irrational, then n is irrational using a proof by contrapositive.

Solution:

5. Proof by Contrapositive I

Prove for all real numbers that if $n^2 + 2$ is irrational, then n is irrational using a proof by contrapositive.

Solution: We will prove the contrapositive, that is: If n is rational, then $n^2 + 2$ is rational.

- Assume n is rational. Then we can write it as $n = \frac{a}{b}$ for arbitrary integers a and b, with $b \neq 0$.
- This means $n^2 + 2 = (\frac{a}{b})^2 + 2$.
  $= \frac{a^2}{b^2} + 2$
  $= \frac{a^2+2b^2}{b^2}$
- Since the integers are closed on addition and multiplication, we can define $c = a^2 + 2b^2$ and $d = b^2$ (and since $b \neq 0$, $b^2 \neq 0$, and therefore $d \neq 0$).
- Therefore, we can say $n^2 + 2 = \frac{c}{d}$, where c and d are integers, and $d \neq 0$.
- Thus from the definition of a rational number, $n^2 + 2$ is rational.

Therefore, by contrapositive we can say that for all real numbers, if $n^2 + 2$ is irrational, then n is irrational.

Problem:

6. Proof by Contrapositive II

Prove or disprove the following statement: for any two integers a, b, if their product ab is even then either a is even or b is even.

Solution:

6. Proof by Contrapositive II

Prove or disprove the following statement: for any two integers a, b, if their product ab is even then either a is even or b is even.

Solution: We will prove this statement.

Proof by Contraposition:
Let a and b be odd.
Then $a = 2k + 1$ and $b = 2c + 1$ for some integers k and c.
$ab = (2k + 1)(2c + 1) = 4kc + 2k + 2c + 1 = 2(2kc + k + c) + 1$
So, ab is odd.
Thus, by contraposition, if ab is even, then a is even or b is even.

Note: this problem can also be solved using a proof by contradiction, which we will talk about next week!