FA 23

EECS 203 Discussion 4

Proof by Contradiction, Proof by Cases

Admin Notes:

Homework:

- Homework/Groupwork 4 was due Sept. 21st
- Homework/Groupwork 5 should be released! It will be due **Sept. 28th**
  - **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 ($\rightarrow$) 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

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:** Proves $p \rightarrow q$ by showing

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

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

  $p \rightarrow p1 \vee p2 \vee \ldots \vee pn \rightarrow q$

Some Methods of Proving $p \to q$

- **Direct Proof:**
  Proves $p \to q$ by showing $\mathbf{p \to stuff \to q}$

- **Proof by Contraposition:**
  Proves $p \to q$ by showing $\mathbf{\neg q \to stuff \to \neg p}$
  (Once you show $\neg q \to \neg p$, you can immediately conclude $p \to q$ 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, $p \to q$.
  $\mathbf{(p \land \neg q) \to F \to \neg(p \land \neg q) \equiv \neg p \lor q \equiv p \to q}$

- **Proof by Cases:**
  Break p into cases and show that each case implies q (in which case $p \to q$).
  $\mathbf{p \to p_1 \lor p_2 \lor \dots \lor p_n \to q}$

Useful Definitions

***Note:** **iff** stands for if and only if ($\leftrightarrow$)

- **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. $\exists x\ [x\neq 1 \land x\neq p \land x|p]$

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]

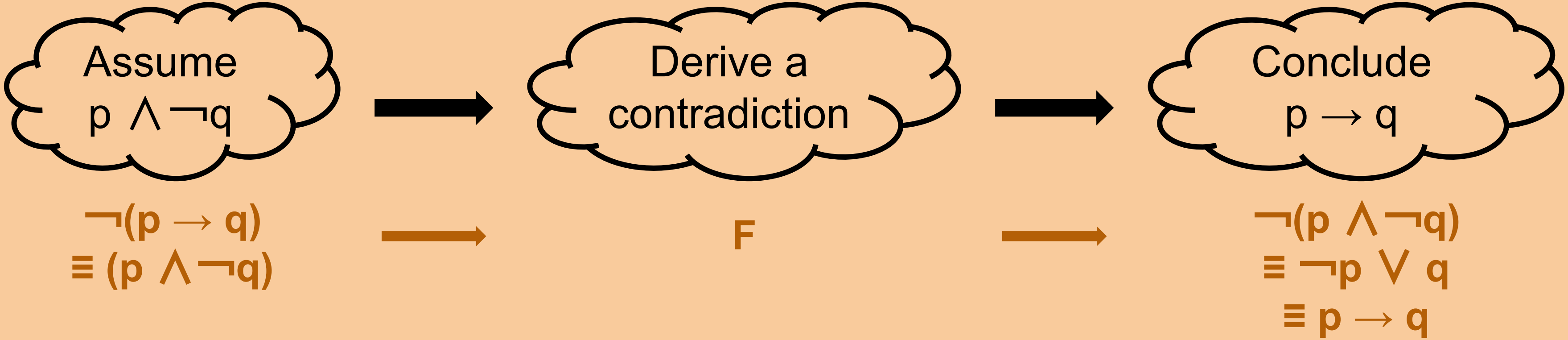
… show that P(x) holds for that value of x.

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

Proof by Contradiction

Proof by Contradiction

- When trying to prove p implies q, assume p is true and q is false. Derive a **contradiction**, (something that is always false, **ex:** $0 = 2$, **ex:** $x = y$ and $x \neq y$). Therefore, $p \rightarrow q$.
    - We assume the negation of what we want to prove
    - We arrive at something false
    - Therefore the negation of the thing we assumed must be true (ie the thing we wanted to prove)



Proof by Contradiction Template

Template: Proof by Contradiction

Claim: p

Proof Template

Seeking a contradiction, assume: [state the negation of p]

… (make some deductions, eventually leading to a contradiction) …

Common contradictions: a number is an **integer and is not an integer**;
a number is both **even and odd**; a number is both **rational and irrational**.

Since *[restate contradictory statements]*, we have a contradiction.
Assuming $\neg p$ led to a contradiction. Therefore, p must be true. (optional concluding sentence)

Special case: when the claim is an "if-then" statement

Claim: $a \to b$

Remember: the negation of $a \to b$ is
a and $\neg b$

Notes:

- **Proof by Contraposition:** Proves p → q by showing
  ¬q → stuff → ¬p
- **Proof by Contradiction:** Proves p → q by showing
  (p ∧¬q) → F → ¬(p ∧¬q) ≡ ¬p ∨ q ≡ p → q

Problem:

1. Contraposition vs Contradiction ⋆

Show that for all integers n, if $n^3 + 5$ is odd, then n is even, using

a) a proof by contraposition.

b) a proof by contradiction.

Note: The algebra in either case is the same. You don't need to rewrite the algebra for part (b), just reformat your proof from (a) into a proof by contradiction.

Solution:

1. Contraposition vs Contradiction ⋆

Show that for all integers n, if $n^3 + 5$ is odd, then n is even, using

a) a proof by contraposition.

b) a proof by contradiction.

Note: The algebra in either case is the same. You don't need to rewrite the algebra for part (b), just reformat your proof from (a) into a proof by contradiction.

Solution:

a) We will prove the contrapositive of the proposition, which is: "if n is odd, then $n^3 + 5$ is even".
Since n is odd, n can be written as $2k + 1$, where k is some integer. Then,

$$\begin{aligned} n^3 + 5 &= (2k+1)^3 + 5 \\ &= (8k^3 + 12k^2 + 6k + 1) + 5 \\ &= 8k^3 + 12k^2 + 6k + 6 \\ &= 2(4k^3 + 6k^2 + 3k + 3) \end{aligned}$$

So $n^3 + 5 = 2m$, where m is the integer $4k^3 + 6k^2 + 3k + 3$. Because $n^3 + 5$ is two times some integer, we can say that $n^3 + 5$ is even.

Solution:

1. Contraposition vs Contradiction $\star$

Show that for all integers n, if n^3+5 is odd, then n is even, using

a) a proof by contraposition.

b) a proof by contradiction.

Note: The algebra in either case is the same. You don't need to rewrite the algebra for part (b), just reformat your proof from (a) into a proof by contradiction.

b) We will use a proof by contradiction. Let n^3+5 be odd. *Seeking a contradiction*, assume that n is odd. Since n is odd, it can be written as $2k+1$, where k is some integer. So

$$\begin{aligned} n^3+5 &= (2k+1)^3+5 \\ &= (8k^3+12k^2+6k+1)+5 \\ &= 8k^3+12k^2+6k+6 \\ &= 2(4k^3+6k^2+3k+3) \end{aligned}$$

Since $n^3+5=2m$, for an integer m ($m=4k^3+6k^2+3k+3$), then n^3+5 is even. Since the premise was that n^3+5 is odd, this completes the contradiction. Therefore, our assumption that n is odd must be false, leading to the conclusion that n is even.

Note:

You can also start this proof by contradiction by assuming the negation of the entire "if ... then" statement. Here, this would entail starting with "Seeking contradiction, assume that n^3+5 is odd and n is odd." From here, the logic of finding a contradiction by showing that n^3+5 is even is almost identical.

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. Odd Proof III

Prove that for all integers a and b, if a divides b and $a + b$ is odd, then a is odd.

Solution:

2. Odd Proof III

Prove that for all integers a and b, if a divides b and $a+b$ is odd, then a is odd.

Solution: Proof by Contradiction

- We are supposed to prove: $[(a \text{ divides } b) \wedge (a+b \text{ is odd})] \rightarrow a$ is odd
- Seeking contradiction, assume the negation of the above statement: $\neg\, [[a \text{ divides } b \wedge a+b \text{ is odd}] \rightarrow a \text{ is odd}]$, which is $(a \text{ divides } b) \wedge (a+b \text{ is odd}) \wedge (a \text{ is even})$.
- Since a is even, $a = 2k$ for some integer k.
- Since a divides b we have $b = m \cdot a$.
- So, $a+b$ becomes $2k+m(a) = 2k+m(2k) = 2(k+km) = 2p$, where p is an integer equal to $k+km$
- Thus $a+b = 2p$ and is even. However, we had originally assumed that $a+b$ is odd. This leads to our **contradiction**.
- Hence the assumption in the second bullet point is false, and $[(a \text{ divides } b) \wedge (a+b \text{ is odd})] \rightarrow a$ is odd

Notes:

- **Rational:** A number **x** is rational iff it can be written as the quotient of two integers. **x = p/q**

Problem:

3. Proof Practice $\star$

Prove or disprove that for all irrational numbers x and rational numbers y, $2x - y$ is irrational.

Solution:

3. Proof Practice ⋆

Prove or disprove that for all irrational numbers x and rational numbers y, $2x - y$ is irrational.

Solution: Proof by Contradiction

We prove the statement via proof by contradiction. Let x be an arbitrary irrational number. Let y be an arbitrary rational number such that $y = \frac{a}{b}$ with a and b as integers and $b \neq 0$. We assume that $2x - y$ is rational, which means that $2x - \frac{a}{b}$ is rational. Then we can write $2x - \frac{a}{b} = \frac{p}{q}$ for some integers p and q with $q \neq 0$. This gives $2x = \frac{p}{q} + \frac{a}{b} = \frac{pb+aq}{bq}$, so $x = \frac{pb+aq}{2bq}$. Note that both the numerator and the denominator are integers, and that $2bq \neq 0$ since b and q were both nonzero. Therefore, x is, by definition, a rational number, which is a contradiction since x was assumed to be irrational. Hence, it must be that the sum of a rational number and an irrational number is irrational.

Proof by Cases

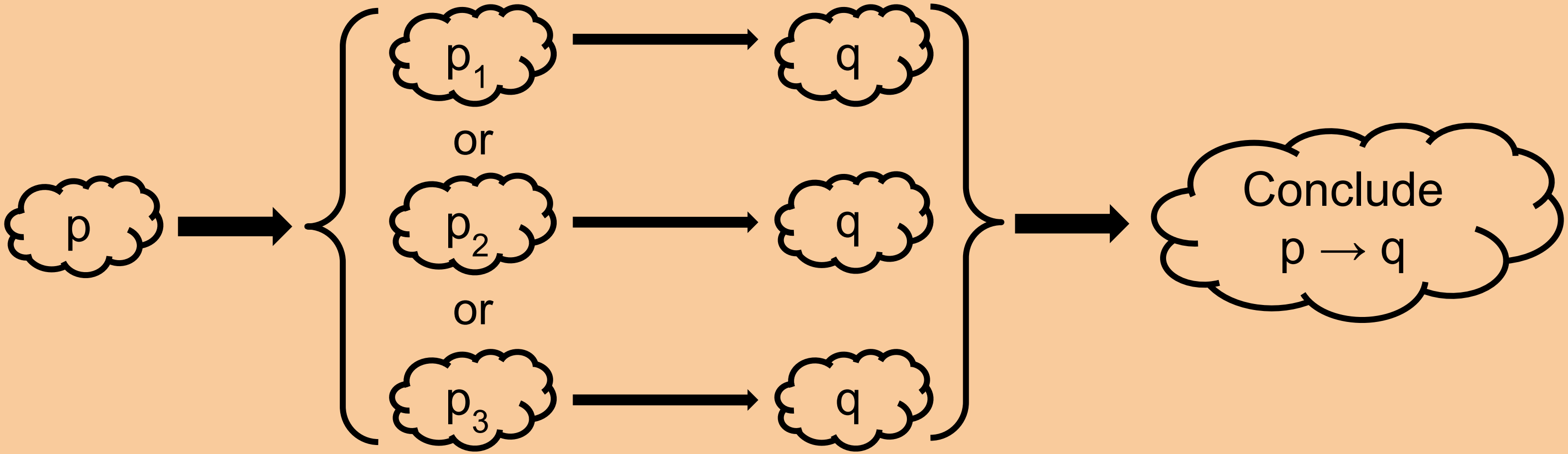
Proof by Cases

Break p into cases and show that each case implies q (in which case $p \rightarrow q$).

$$p \rightarrow p_1 \lor p_2 \lor \ldots \lor p_n \rightarrow q$$

$p_1 \lor p_2 \lor \ldots \lor p_n$ should cover all possible cases for p.

- We break our statement into all possible cases
- We show that each case leads to the conclusion we want



Proof by Cases Template

Proof by cases (at top level)

Given: p_1 or p_2 or ...

Claim: q

Often this isn't explicitly given, but rather something we know (e.g., a number is either even or odd; positive, negative, or zero; etc.)

Proof

- Proof by cases:
    - **case 1:** Assume p_1.
    - *...(deductions)...*
    - q.

    - **case 2:** Assume p_2.
    - *...(deductions)...*
    - q

    - ...
- Thus, q.

Notes:

- **Rational:** A number **x** is rational iff it can be written as the quotient of two integers. **x = p/q**

Problem:

4. Polynomial Proof $\star$

Prove that there does not exist a rational number x satisfying the equation $x^3 + x + 1 = 0$.
Hint: Use the fact that 0 is an even number.
You can use the following lemmas without proving:

- Odd $\times$ Even $=$ Even
- Odd $\times$ Odd $=$ Odd
- Even $\times$ Even $=$ Even
- Odd $+$ Even $=$ Odd
- Odd $+$ Odd $=$ Odd
- Even $+$ Even $=$ Even

Solution:

4. Polynomial Proof ⋆

Prove that there does not exist a rational number x satisfying the equation $x^3 + x + 1 = 0$.
Hint: Use the fact that 0 is an even number.
You can use the following lemmas without proving:

Solution:
Suppose there is. Let a solution be $\frac{a}{b}$, with a, b in reduced form.
Then we know that $\frac{a^3}{b^3} + \frac{a}{b} + 1 = 0 \iff a^3 + ab^2 + b^3 = 0$.
Since the RHS is even, LHS should be even as well.

Case 1: a, b both odd.
Then we have LHS = odd + odd × odd + odd = odd.
Case 2: a is odd, b is even.
Then we have LHS = odd + even + even = odd.
Case 3: a is even, b is odd.
(note that WLOG does not apply here since a, b are not symmetric; there is a term ab^2).
Then we have LHS = even + even + odd = odd.
Case 4: a, b are both even.
This cannot occur since a, b is in reduced form.

Each case results in LHS being odd which is a contradiction if LHS = 0. Thus we have proved by contradiction that the equation $x^3 + x + 1$ has no solution in $\mathbb{Q}$.

Notes:

- **Prime:** A prime number **p** is a number greater than 1 whose only factors are 1 and itself. **$\forall x\ [x|p \rightarrow (x=1 \lor x=p)]$**

Problem:

5. Prime Proof ⋆

Show that for any prime number p, $p^2 + 11$ is composite (not prime). Recall that a prime p is defined to be a positive integer ≥ 2 such that p and 1 are the only positive integers that divide p.

Solution:

5. Prime Proof ⋆

Show that for any prime number p, $p^2 + 11$ is composite (not prime). Recall that a prime p is defined to be a positive integer ≥ 2 such that p and 1 are the only positive integers that divide p.

Solution: We can consider two cases: either p is even, or it is odd.

- Case 1: Consider the even primes, which is just $p = 2$. $p^2 + 11 = 15$, and $15 = 5 \cdot 3$ is composite.

- Case 2: Now we consider the odd primes, or any prime greater than 2. Since p is odd, we have $p = 2k + 1$ for some integer $k > 1$. Then

$$p^2 + 11 = (2k + 1)^2 + 11 = 4k^2 + 4k + 12 = 2(2k^2 + 2k + 6).$$

  Hence, $p^2 + 11$ can be factored into 2 and $2k^2 + 2k + 6$, therefore $p^2 + 11$ is composite.

We have exhausted all non-overlapping cases and proved that for all primes p, $p^2 + 11$ is composite.

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** $\neg(P \rightarrow Q) \equiv \neg(\neg P \lor Q) \equiv (P \land \neg Q)$

Problem:

6. Rational Proof $\star$

1. Prove or disprove: For all nonzero rational numbers x and y, x^y is rational
2. Prove or disprove: For all nonzero integers x and y, x^y is rational

Solution:

6. Rational Proof ⋆

1. Prove or disprove: For all nonzero rational numbers x and y, x^y is rational
2. Prove or disprove: For all nonzero integers x and y, x^y is rational

Solution:

1. This is false. Let $x = 2$ and $y = \frac{1}{2}$. Then $x^y = \sqrt{2}$ which is irrational.
2. This is true. We prove this by cases. Case 1: $y > 0$ Then x^y is x multiplied by itself y times - and thus x^y is an integer. As we know all integers are rational, x^y must be rational. Case 2: $y < 0$ Then $x^y = \frac{1}{x^{-y}}$. As $y < 0$, $-y > 0$ so x^{-y} is an integer. As both 1 is an integer, and x^{-y} is an integer, we know $\frac{1}{x^{-y}}$ is rational.

Problem:

7. Proving the Triangle Inequality

Prove the triangle inequality, which states that for all real numbers x and y, we have $|x| + |y| \geq |x + y|$ (where $|x|$ represents the absolute value of x, which equals x if $x \geq 0$ and equals $-x$ if $x < 0$).

Solution:

Solution: This is a proof by cases. There are 4 cases to consider:

- x and y are both nonnegative
- x and y are both negative
- $x \geq 0$, $y < 0$, $x \geq -y$
- $x \geq 0$, $y < 0$, $x < -y$

Since x and y play symmetric roles (you can switch the values of x and y without impacting the validity of the triangle inequality), we can assume without loss of generality (WLOG) for the last two cases that $x \geq 0$ and $y < 0$.

- Case 1: If x and y are both nonnegative, then $|x| + |y| = x + y = |x + y|$.
- Case 2: If x and y are both negative, then $|x| + |y| = (-x) + (-y) = -(x + y) = |x + y|$.
- Case 3: If $x \geq 0$ and $y < 0$ and $x + y \geq 0$, then $|x| + |y| = x + (-y)$ is some number greater than x. $|x + y|$ is some positive number less than x since y is negative. Thus, $|x| + |y| \geq x \geq |x + y|$.
- Case 4: If $x \geq 0$ and $y < 0$ and $x + y < 0$, then $|x| + |y| = x + (-y)$ is some number greater than $-y$. $|x + y| = -(x + y) = (-x) + (-y)$ which is some positive number less than or equal to $-y$, since $-x$ is nonpositive. Thus, we have $|x| + |y| \geq -y \geq |x + y|$.

We have now proved for all cases that the triangle inequality is valid. This example is purposely lengthy to show in full detail a proof by cases.