HW07

Sam Ly

October 23, 2025

Total points: 22

Required Exercise 1 [4]

Prove or disprove the following:

1. [1] There exists a pair of rational numbers $a, b \in \mathbb{Q}$ with $a < b$ such that there is no $c \in \mathbb{Q}$ with $a < c < b$.

   Proof. We see that for every pair of rational numbers $a, b \in \mathbb{Q}$, we can create a new rational number $\frac{a+b}{2}$.

   Then, if $a < b$, we see that $a < \frac{a+b}{2} < b$. Therefore, we have contradicted our original proposition, disproving the original claim. □

2. [1] For all natural numbers $n \in \mathbb{N}$, such that $29 \nmid n$, $2n^2 + 29$ is prime.

   Proof. One counter-example to this claim is $n = 29$. This is because when $n = 29$, we get

   $$2(29)^2 + 29$$

   $$29(2(29) + 1).$$

   This number is a product of 29 and $2(29) + 1$, meaning it is not prime. Therefore, we have disproven our original claim. □

3. [1] Let n be an integer, then $10 \mid n$ if and only if $100 \mid n^3$.

   Proof. We begin by seeing that our proposition is equivalent to saying that $10 \mid n$ implies $100 \mid n^3$ and $100 \mid n^3$ implies $10 \mid n$.

   We continue by first proving $10 \mid n \Rightarrow 100 \mid n^3$.

   By using modular arithmetic, we see:

   $$\begin{aligned} n &\equiv 0 \pmod{10} \\ n^2 &\equiv 0 \pmod{100} \\ n^3 &\equiv 0 \pmod{1000}. \end{aligned}$$

   Since $100 \equiv 0 \pmod{1000}$ and $n^3 \equiv 0 \pmod{1000}$, $n^3 \equiv 0 \pmod{100}$. So, $100 \mid n^3$.

   Therefore, $n \mid 10 \Rightarrow n^3 \mid 100$.

   Now, to see that $100 \mid n^3 \Rightarrow 10 \mid n$, we first suppose $100 \mid n^3$. Then, we see that $4 \mid n^3$ and $25 \mid n^3$.

   Thus, $2 \mid n^3$ and $2 \mid n$. Also, $5 \mid n^3$ and $5 \mid n$.

   Since $2 \mid n$ and $5 \mid n$, $10 \mid n$.

   Therefore, $10 \mid n$ if and only if $100 \mid n^3$. □

4. [2] The square root of 2 is rational: $\sqrt{2} \in \mathbb{Q}$.

   Proof. We begin by assuming that $\sqrt{2}$ is rational, and thus is can be written in the form $\frac{a}{b}$ for $a, b \in \mathbb{Z}$ in lowest terms. Because $\frac{a}{b}$ is in lowest terms, they can not both be even.

   Now, we see

$$\begin{aligned}\sqrt{2} &= \frac{a}{b}\\ 2 &= \frac{a^2}{b^2}\\ b^2 &= \frac{a^2}{2}.\end{aligned}$$

   Since b^2 is an integer, a^2 must be even. Since an odd number squared is always odd, and an even number squared is always even, a must be even. Thus, $a = 2n$, for $n \in \mathbb{Z}$. By substituting, we see

$$b^2 = \frac{(2n)^2}{2} = \frac{4n^2}{2} = 2n^2,$$

   meaning b^2 is even and b is even.

   We previously assumed that $\frac{a}{b}$ was in lowest terms, and thus can not both be even. Because we have arrived at a contradiction, we can conclude that $\sqrt{2}$ is not rational. □

Required Exercise 2 [3]

Done! See below.

Required Exercise 3 [2]

One "stupid proof trick" is that quantified statements follow their own form of De Morgan's Laws. For example, when we say "For all students s at CPP, s has a unique student ID." we can also say that "There does not exist a student s at CPP, where s has a preexisting student ID."

This is one of the rare cases where the formal notation for quantified logical statements is useful because it lets us "see" the algebraic structure easier.

Let P be some arbitrary logical statement, and $\mathcal{U}$ be the universal set. We see that:

$$\begin{aligned}\forall x \in \mathcal{U}, P &\Leftrightarrow \neg(\exists x \in \mathcal{U}, \neg P)\\ \exists x \in \mathcal{U}, P &\Leftrightarrow \neg(\forall x \in \mathcal{U}, \neg P).\end{aligned}$$

Required Exercise 4 [1]

1. Done! I explicitly state that our proof will be inductive, and clarified some structural elements.

2. I found the feedback very helpful. I like how simple and immediately implementable the feedback is.

Choice Exercise 6 [3]

1. In the first required exercise, you proved that $\sqrt{2}$ is irrational. Use a similar idea to prove that the square root of 3 is irration: that is, $\sqrt{3} \notin \mathbb{Q}$.

   Proof. We proceed by contradiction. First we assume that $\sqrt{3}$ is rational, and thus can be written in the form a/b for $a, b \in \mathbb{N}$ in lowest terms. Since a and b are in lowest terms, they can not both be divisible by 3.

   Using algebraic manipulation, we see:

$$\begin{aligned} \sqrt{3} &= \frac{a}{b} \\ 3 &= \frac{a^2}{b^2} \\ b^2 &= \frac{a^2}{3}. \end{aligned}$$

   Since b^2 is an integer, $3 \mid a^2$, and by extension $3 \mid a$. Thus, $a = 3n$ for some integer n. By substituting, we see:

$$\begin{aligned} b^2 &= \frac{(3n)^2}{3} \\ b^2 &= \frac{9n^2}{3} \\ b^2 &= 3n^2. \end{aligned}$$

   Thus, $3 \mid b^2$, and by extension, $3 \mid b$. Therefore, we have arrived at a contradiction, so $\sqrt{3}$ is not rational. □

Choice Exercise 7 [3]

Prove that if $\star \colon X \times X \to X$ is a binary operation and $a \star b = b \star a$ for all $a, b \in X$, then

$$a_1 \star a_2 \star \cdots \star a_n = a_n \star \cdots \star a_2 \star a_1$$

for all positive integers $n \in \mathbb{Z}$.

Proof. We proceed via induction. For our base cases, we see that our relation holds true for $n = 2$:

$$a_1 \star a_2 = a_2 \star a_1.$$

As an inductive hypothesis, we assume

$$a_1 \star a_2 \star \cdots \star a_n = a_n \star \cdots \star a_2 \star a_1$$

holds for $n \leq k$.

Thus, we have

$$a_1 \star a_2 \star \cdots \star a_k = a_k \star \cdots \star a_2 \star a_1.$$

Then, for $n = k + 1$ we have:

$$\begin{aligned} &a_1 \star a_2 \star \cdots \star a_k \star a_{k+1} \\ &= a_{k+1} \star (a_1 \star a_2 \star \cdots \star a_k). \end{aligned}$$

Then, from our inductive hypothesis, we substitute to get:

$$= a_{k+1} \star a_k \star \cdots \star a_2 \star a_1.$$

Thus, for any binary operation $\star : X \times X \to X$ such that $a \star b = b \star a$ for all $a, b \in X$, then

$$a_1 \star a_2 \star \cdots \star a_n = a_n \star \cdots \star a_2 \star a_1$$

for all positive integers $n \in \mathbb{Z}$. □

Choice Exercise 10 [6]

1. [1] Give examples of the following:
   - All 5 words (of length 3) that begin with a and begin with a non-trivial palindrome.

     $$aaa, aab, aac, aba, aca.$$

   - All 4 words that begin with a but do not begin with a non-trivial palindrome.

     $$abb, abc, acc, acb.$$

   - A 7-letter word that does not begin with a non-trivial palindrome.

     $$abcabca.$$

2. [1] perhaps my first original proof was that the number of such words of length n was given by the formula

   $$\begin{aligned} &a(0) = a(1) = 0, \text{ and} \\ &a(n) = 3a(n-1) + 3^{\lceil n/2 \rceil} - a(\lceil n/2 \rceil) \text{ for } n \geq 2, \end{aligned}$$

   where if $x \in \mathbb{R}$ then the *ceiling* of x is written $\lceil x \rceil$ and is the least ineger greater than or equal to x.

   - Compute (by hand) $\lceil 3.1415926 \rceil$, $\lceil 3100 \rceil$, and $\lceil -9.19 \rceil$.

     $$\begin{aligned} \lceil 3.1415926 \rceil &= 4 \\ \lceil 3100 \rceil &= 3100 \\ \lceil -9.19 \rceil &= -9. \end{aligned}$$

   - Start a stopwatch, and try to write a computer program that will compute $a(26) = 1833980928771$.

```
from functools import cache
from math import ceil


@cache
def a(n: int):
    if n == 0 or n == 1:
        return 0

    return 3 * a(n-1) + 3**ceil(n/2) - a(ceil(n/2))

print("a(26) = ", a(26))
# a(26) =  1833980928771
```

3. [4] Recursion and induction are essentially the same idea. Use induction to prove that the formula is correct.

Proof. We proceed with mathematical induction. We see that for our base cases $n = 0, 1$, there are no such strings that satisfy our condition because there are no non-trivial palindromes of length 0 or 1. So, $a(0) = a(1) = 0$.

For our inductive hypothesis, we assume

$$a(n) = 3a(n-1) + 3^{\lceil n/2 \rceil} - a(\lceil n/2 \rceil) \text{ for } 2 \leq n \leq k.$$

For $n = k + 1$, we have

$$a(k+1) = 3a(k) + 3^{\lceil k/2 \rceil} - a(\lceil k/2 \rceil).$$

We arrive at this conclusion by seeing that when we increase our string length by 1, we can:

(a) append a, b, or c to the end of a previously valid string to create a new valid string.

(b) create a new palidrome of length $k + 1$ that begins with a.

However, see that there are certain strings that are being counted twice between these two cases. For example, $aaa \ldots a$ can be created from both case (a) and (b).

Specifically, the strings that are counted twice are the strings that are both fully a palindrome, and contain a subpalindrome. The only way for this to happen is if the first half of the string contains a palindrome.

Thus, our inductive step holds. Therefore, by induction, the n'th term of our sequence is

$$a(n) = 3a(n-1) + 3^{\lceil n/2 \rceil} - a(\lceil n/2 \rceil) \text{ for } 2 \leq n \leq k.$$

□

Proofs Portfolio

MAT 3100W: Intro to Proofs

Sam Ly

October 23, 2025

1 Introduction

(Leave this blank for now. Here's an outline of course topics for your reference.)

2 Mathematical concepts

2.1 Logical Statements

Definition 1. A logical statement is a statement that can either be **true** or **false**. Logical statements must be unambiguous, meaning all ratioal agents with access to the same information will come to the same conclusion.

Proposition 1. *"The sun rose today." is a* ***true*** *logical statement.*

Proof. We begin by observing that the we can currently see the sun in the sky and that we could not see the sun in the sky last night. If we can not see the sun in the sky, it must be below the horizon. Because the sun follows a continuous path, and it had been below the horizon last night, it must have crossed the horizon at some point between last night and now. Thus the sun must have risen today. □

3 Proof techniques

3.1 Direct Proofs

Suppose $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$. Prove the following:

1. $a + b \equiv a' + b' \pmod{m}$.

   Proof. We begin with by defining $a \equiv a' \pmod{m}$ as $m \mid (a - a')$. Similarly, $m \mid (b - b')$.

   Following from these definitions, we write:

   $$a - a' = m \times k_1 \tag{1}$$

   $$b - b' = m \times k_2 \tag{2}$$

   We can add equations 1 and 2 together to get $a + b - a' - b' = m \times k_1 + m \times k_2$.

   With some factoring, we get $(a + b) - (a' + b') = m(k_1 + k_2)$.

   By definition, we find that $m \mid (a + b) - (a' + b')$, and thus $a + b \equiv a' + b' \pmod{m}$. □

2. $a - b \equiv a' - b' \pmod{m}$.

Proof. Following from Proof 1, we can instead subtract equation 1 and 2 to get $a - b - a' + b' = m \times k_1 - m \times k_2$.

With some factoring, we get $(a - b) - (a' - b') = m(k_1 - k_2)$.

By definition, we find that $m \mid (a - b) - (a' - b')$, and thus $a - b \equiv a' - b' \pmod{m}$. □

3. $a \times b \equiv a' \times b' \pmod{m}$.

Proof. Following from equation 1, we get

$$a = a' + m \times k_1. \tag{3}$$

Similarly, from equation 2, we get

$$b = b' + m \times k_2. \tag{4}$$

By multiplying equations 3 and 4, we get $a \times b = (a' + m \times k_1)(b' + m \times k_2)$.

From now on, I will omit the × symbol.

By distributing, we get

$$ab = a'b' + a'mk_2 + b'mk_1 + m^2k_1k_2.$$

We can factor out m to find

$$ab = a'b' + m(a'k_2 + b'k_1 + mk_1k_2).$$

We can subtract $a'b'$ from both sides to find

$$ab - a'b' = m(a'k_2 + b'k_1 + mk_1k_2).$$

By definition, we see that $m \mid (ab - a'b')$, and, by extension, $ab \equiv a'b' \pmod{m}$.

□

3.2 Proof by Induction

As an example of Proof by Induction, we will prove the following.

Proposition 2. *Show that every positive integer is a sum of one or more numbers of the form 2^r3^s, where r and s are nonnegative integers and no summand divides another. (For example, $23 = 9 + 8 + 6$).*

Proof. We proceed by mathematical induction.

We start with $n = 0, 1$ as our base cases. We see that $n = 0$ is true, and $n = 1$ is true because $1 = 2^03^0$.

Now, we create the inductive hypothesis that all nonnegative integers strictly less than n have such summation.

If n is even, we can construct a valid summation by noticing that, from our inductive hypothesis, $\frac{n}{2}$ has a valid summation $\sum_{i=1}^{k} 2^{r_i}3^{s_i}$. Since none of these summands divide any other summand, multiplying all summands by 2 also creates a set of summands such that no summand divides another.

If n is odd, we can also construct a valid summation by picking a value 3^t that is the biggest power of 3 that is less than or equal to n. Our proposition is trivially true if $n = 3^t$. Otherwise, we must find a value $m = n - 3^t$.

Since n and 3^t are both odd, m must be even. Also notice that $m < n$. Thus, there must exist a valid summation $m = \sum_{j=1}^{k} 2^{r_j}3^{s_j}$ where all $r_j \geq 1$.

Since all summands of m are even, 3^t can not be divisible by any of the summands of m. Also, since $r_j \geq 1$, there must not be any summand where $s_j \geq t$ because if such summand existed, we would find at least a value of $n = 3^t + 2(3^t) = 3^{t+1}$. This is a contradiction, since we defined 3^t as the largest power of 3 less than or equal to n.

Thus, $n = \sum 2^r3^s$ where no summand divides another for all nonnegative integers n. □

Proposition 3. *Let F_n be the n-th Fibonacci number, where $F_0 = F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$. Prove that $F_n \leq 1.9^n$ for all $n \geq 1$.*

Proof. We proceed by induction, starting with the base cases, where $n = 1, 2$:

$$n = 1, F_1 = 1 \leq 1.9^1 = 1.9$$

$$n = 2, F_2 = 2 \leq 1.9^2 = 3.61.$$

We assume as an inductive hypothesis that $F_n \leq 1.9^n$ for $1 \leq n \leq k$.
Using our inductive hypothesis, we see that $F_k \leq 1.9^k$ and $F_{k-1} \leq 1.9^{k-1}$.
So, $F_k + F_{k-1} \leq 1.9^k + 1.9^{k-1}$.
By refactoring $1.9^k + 1.9^{k-1}$, we get:

$$1.9^k + 1.9^{k-1} = 1.9(1.9^{k-1}) + 1.9^{k-1} = 2.9(1.9^{k-1}).$$

Also, 1.9^{k+1} can be rewritten as $1.9^2(1.9^{k-1}) = 3.61(1.9^{k-1})$.
Finally, we see

$$F_{k+1} = F_k + F_{k-1} \leq 2.9(1.9^{k-1}) \leq 3.61(1.9^{k-1}) = 1.9^{k+1}$$

$$F_{k+1} \leq 1.9^{k+1}.$$

Thus, we conclude that by the principle of mathematical induction, $F_n \leq 1.9^n$ for all $n \geq 1$. □

Proposition 4. *Look up the Tower of Hanoi puzzle. Prove that given a stack of disks, you can solve the puzzle in moves.*

Proof. We begin by defining the Tower of Hanoi problem.

In this problem, we begin with a stack of n disks. The disks are ordered from largest at the bottom to smallest at the top. We are also given 3 'spots' to place our disks under one condition: that we never place a larger disk on top of a smaller disk.

Following these rules, what is the minimum number of moves required to move the entire pile to a new 'spot'?

We define the function $f : \mathbb{N} \to \mathbb{N}$ such that it maps the starting stack height n to the minimum number of moves required to move the entire pile $f(n)$.

Before immediately proving that $f(n) = 2^n - 1$, it is more intuitive to first define f as a recurrence relation, then prove that the recurrence relation is equal to $2^n - 1$.

We notice that moving the entire pile of n disks essentially requires 3 'phases':

1. Moving the top $n - 1$ disks onto a single pile.

2. Moving the nth disk to another vacant spot.

3. Moving the top $n - 1$ disks onto the new spot.

Thus, we know that $f(n) = f(n-1) + 1 + f(n-1) = 1 + 2f(n-1)$, where $f(1) = 1$. We can then prove $f(n) = 2^n - 1$ using induction.

We begin with our base cases:

n	$f(n)$
1	$1 = 2^1 - 1$
2	$3 = 2^2 - 1$
3	$7 = 2^3 - 1$

Now, we assume that $f(k) = 2^k - 1$ for all $1 \leq k \leq n$.
We see that

$$f(k+1) = 1 + 2f(k)$$

$$f(k+1) = 1 + 2(2^k - 1)$$

$$f(k+1) = 2^{k+1} - 1.$$

Thus, $f(n) = 2^n - 1$. □

4 Final project

5 Conclusion and reflection

Appendix

(The first section, "Course objectives and student learning outcomes" is just here for your reference.)

A Course objectives and student learning outcomes

1. Students will learn to identify the logical structure of mathematical statements and apply appropriate strategies to prove those statements.
2. Students learn methods of proof including direct and indirect proofs (contrapositive, contradiction) and induction.
3. Students learn the basic structures of mathematics, including sets, functions, equivalence relations, and the basics of counting formulas.
4. Students will be able to prove multiply quantified statements.
5. Students will be exposed to well-known proofs, like the irrationality of $\sqrt{2}$ and the uncountability of the reals.

A.1 Expanded course description

- Propositional logic, truth tables, DeMorgan's Laws
- Sets, set operations, Venn diagrams, indexed collections of sets
- Conventions of writing proofs
- Proofs
  - Direct proofs
  - Contrapositive proofs
  - Proof by cases
  - Proof by contradiction
  - Existence and Uniqueness proofs
  - Proof by Induction
- Quantifiers
  - Proving universally and existentially quantified statements
  - Disproving universally and existentially quantified statements
  - Proving and disproving multiply quantified statements
- Number systems and basic mathematical concepts
  - The natural numbers and the integers, divisibility, and modular arithmetic
  - Counting: combinations and permutations, factorials
  - Rational numbers, the irrationality of $\sqrt{2}$
  - Real numbers, absolute value, and inequalities
- Relations and functions
  - Relations, equivalence relations
  - Functions
  - Injections, surjections, bijections

- Cardinality
  - Countable and uncountable sets
  - Countability of the rational numbers, $\mathbb{Q}$
  - Uncountability of the real numbers, $\mathbb{R}$