

HW08

Sam Ly

November 3, 2025

Total points = 18

Required Exercise 1 [4]

1. Done. See below.
2. Add definitions for all subsections of section 2.
3. DNF.
4. DNF.
5. Done. See below.

Required Exercise 2 [2]

Suppose that A_1, A_2, \dots, A_{n+1} is a collection of sets and f_1, f_2, \dots, f_n is a collection of functions such that $f_i : A_i \rightarrow A_{i+1}$ for all $i \in \{1, 2, \dots, n\}$.

Let \circ denote the composition of functions so that $(g \circ h)(x) = g(h(x))$.

1. Explain why $f_1 \circ f_2$ is not well-defined.

For a composition $f_a \circ f_b$ to be well-defined, the codomain of f_b must be the same as the domain of f_a . We see that $f_2 : A_2 \rightarrow A_3$, so the codomain of f_2 is A_3 . However, we see that $f_1 : A_1 \rightarrow A_2$, so the domain of f_1 is A_1 . Since $A_1 \neq A_3$, $f_1 \circ f_2$ is not well-defined.

2. Explain why $f_2 \circ f_1$ is well-defined.

We see that $f_1 : A_1 \rightarrow A_2$ and $f_2 : A_2 \rightarrow A_3$. The codomain of f_1 is A_2 , which is the same as the domain of f_2 . Thus, $f_2 \circ f_1$ is well-defined.

3. Prove that $f_n \circ f_{n-1} \circ \dots \circ f_2 \circ f_1$ is a well-defined function, and state its domain and codomain.

Proof. We proceed via induction. As our base case, we see that $f_2 \circ f_1$ is well-defined.

For our inductive hypothesis, we assume that $f_n \circ f_{n-1} \circ \dots \circ f_2 \circ f_1$ is well-defined for $n \leq k$.

Because $g = f_k \circ f_{k-1} \circ \dots \circ f_2 \circ f_1$ is well-defined, and the codomain of f_k is A_{k+1} , we see that $f_{k+1} \circ g$ is also well-defined.

Thus, by the principle of mathematical induction, we see that $f_n \circ f_{n-1} \circ \dots \circ f_2 \circ f_1$ is well-defined. \square

We see that because $f_i : A_i \rightarrow A_{i+1}$, the domain of f_1 is A_1 , and the codomain of f_n is A_{n+1} . Thus, the domain of our entire composed function is A_1 and the codomain is A_{n+1} .

Required Exercise 3 [4]

1.
 - (a) Three examples of integers that are in $3\mathbb{Z} + 2$ would be 2, 5, and 8.
 - (b) The equivalence class an integer n belongs to is determined by its $\pmod{3}$ value.
Integer n belongs to $3\mathbb{Z} + j$ if $3 \equiv j \pmod{3}$ for $j \in \{0, 1, 2\}$.
 - (c) I know that every number is in exactly one of these equivalence classes because 1) the nature of modular arithmetic, and 2) the definition of an equivalence relation.
 - 1) In modular arithmetic, each value maps to exactly one value for any mod value we chose.
 - 2) Equivalence are transitive. Now, if we assume that an element is simultaneously in two equivalence classes A and B , we run into a contradiction since all elements in class A would now also be in class B . Thus, A and B are the same equivalence class.

2. Now let $X = \{1, 2, 3, 4\}$ and let

$$R = \{(1, 1), (1, 2), (1, 4), (2, 1), (2, 2), (2, 4), (3, 3), (4, 1), (4, 2), (4, 4)\},$$

which is to say that for $a, b \in X$, aRb if and only if $(a, b) \in R$.

- Prove that R is an equivalence relation.

Proof. For a relation to be an equivalence relation, it must be reflexive, symmetric, and transitive. We see that R is reflexive since for all $a \in X$, $(a, a) \in R$. That is, all elements are related to themselves.

We also see that R is symmetric because for all $(a, b) \in R$, $(b, a) \in R$ where $a, b \in X$.

Lastly, we see that R is transitive because for all $a, b, c \in X$, if $(a, b) \in R$ and $(b, c) \in R$, $(a, c) \in R$. Thus, R is an equivalence relation. \square

3.
 - Describe the two equivalence classes of X .
3 is in a class of its own, while $\{1, 2, 4\}$ are in another class.
 - Prove that if R_1 is not reflexive, then R_1 does not partition X into equivalence classes.

Proof. We see that for a relation to partition a set into equivalence classes, all elements must belong to an equivalence class. However, since R_1 is not reflexive, we see that there may be an element that does not belong to its own equivalence class. This is a contradiction, thus R_1 can not partition X into equivalence classes. \square

- Prove that if R_2 is not symmetric, then R_2 does not partition X into equivalence classes.

Proof. We proceed via contradiction by assuming that R_2 is not symmetric and that it does partition X into equivalence classes. Since R_2 is not symmetric, there must be an element $(a, b) \in R$ where $(b, a) \notin R$ for $a, b \in X$. This means that there is an element a that is in the same class as b , but b is not in the same class as a . This is a contradiction, so R_2 must not partition X into equivalence classes. \square

- Prove that if R_3 is not transitive, then R_3 does not partition X into equivalence classes.

Proof. We proceed via contradiction by assuming that R_3 is not transitive and that it does partition X into equivalence classes. Since R_3 is not transitive, there are elements $a, b, c \in X$ where aRb and bRc , but $\neg aRc$. This means that a and b are in the same class, and b and c are the same class. But a and c are not in the same class. This is a contradiction, so R_3 must not partition X into equivalence classes. \square

Choice Exercise 8 [6]

1. The sum of a rational number and an irrational number is irrational.

Proof. We proceed by contradiction. Assume that the sum of a rational number a and an irrational number b is rational. Thus, $a + b = c/d$ for $c, d \in \mathbb{N}$.

Now, we see that since $c \in \mathbb{N}$, $c = c_1 + c_2$ for some $c_1, c_2 \in \mathbb{N}$. Thus,

$$\begin{aligned} a + b &= \frac{c}{d} \\ &= \frac{c_1 + c_2}{d} \\ &= \frac{c_1}{d} + \frac{c_2}{d}. \end{aligned}$$

This is a contradiction because it shows that both a and b are rational. Thus, the sum of a rational number and an irrational number is irrational. \square

Proof. We proceed by contrapositive. First, we see that our proposition can be reworded as “If a is rational and b is irrational, then $a + b$ is irrational.”

Thus, the contrapositive of this statement is “If $a + b$ is rational, then a is irrational or b is rational.”

First, we see that $a + b = c/d$ for some $c, d \in \mathbb{N}$. Since $c \in \mathbb{N}$, $c = c_1 + c_2$ for some $c_1, c_2 \in \mathbb{N}$. Thus,

$$\begin{aligned} a + b &= \frac{c}{d} \\ &= \frac{c_1 + c_2}{d} \\ &= \frac{c_1}{d} + \frac{c_2}{d}. \end{aligned}$$

We now see that b is rational. Thus, the sum of a rational number and an irrational number is irrational. \square

2. Suppose a, b and c are positive real numbers. If $ab = c$ then $a \leq \sqrt{c}$ or $b \leq \sqrt{c}$.

Proof. We proceed via contradiction. Assume that $ab = c$ and $a > \sqrt{c}$ and $b > \sqrt{c}$.

Since $a > \sqrt{c}$ and $b > \sqrt{c}$, $ab > \sqrt{c}\sqrt{c} = c$.

This is a contradiction, so $ab = c$ implies $a \leq \sqrt{c}$ or $b \leq \sqrt{c}$. \square

Proof. We proceed via contrapositive. We reword our proposition as “If $a > \sqrt{c}$ and $b > \sqrt{c}$, then $ab \neq c$.”

Since $a > \sqrt{c}$ and $b > \sqrt{c}$, $ab > \sqrt{c}\sqrt{c} = c$. Thus, $ab \neq c$. So, via contrapositive, we see $ab = c$ implies $a \leq \sqrt{c}$ and $b \leq \sqrt{c}$. \square

3. Suppose that n is a composite integer, then there exists a prime divisor of n that is less than or equal to \sqrt{n} .

Proof. We proceed via contradiction. Assume that n is a composite integer, and there does not exist a prime divisor of n that is less than or equal to \sqrt{n} .

Notice that for all integers $a, b > \sqrt{n}$, $ab > n$. Thus, there must be no prime divisors of n , meaning n is prime.

This is a contradiction, so there exists a prime divisor of n that is less than or equal to \sqrt{n} . \square

Proof. We proceed via contrapositive. We reword our proposition as “If there does not exist a prime divisor of n that is less than or equal to \sqrt{n} , then n is prime.”

Notice that for all integers $a, b > \sqrt{n}$, $ab > n$. Thus, there can not exist any prime divisors of n greater than \sqrt{n} .

Also, because there does not exist a prime divisor of n that is less than or equal to \sqrt{n} , there does not exist any prime divisors of n . Thus, n is prime. \square

Choice Exercise 10 [8]

- [1] Compute by hand the number of relations on a set X where $|X| = n$.

All relations are a subset of the $X \times X$. Thus, the number of possible relations is the cardinality of the powerset of X^2 . Thus, the number of possible relations is 2^{n^2} .

- [2] Compute by hand the number of relations that are symmetric but not reflexive on a set X where $|X| = n$.

We first compute the number of relations that are symmetrical. We do this by taking the noticing that this essentially takes the “upper triangle” of our cartesian product because we must include the “other half”.

We get the formula as $n^2 - (n-1)^2 + (n-2)^2 \dots = \sum_{i=0}^n (n-i)^2 (-1)^i$. Now, we find the cardinality of the powerset of a set with said number of elements. Thus, we have the formula $2^{\sum_{i=0}^n (n-i)^2 (-1)^i}$. I later found out that the formula for the number of elements in the “upper triangle” is actually just $\frac{n(n+1)}{2}$. So, a simpler formula would be $2^{\frac{n(n+1)}{2}}$.

Now, the number of symmetric and reflexive relations is sampled from the “lower triangle” because the diagonal is implicitly selected. The formula for this is $\frac{n(n-1)}{2}$. Similarly, all possible relations would be $2^{\frac{n(n-1)}{2}}$.

Finally, we get $2^{\frac{n(n+1)}{2}} - 2^{\frac{n(n-1)}{2}}$ as the formula for the number of relations on set X that is symmetric and not reflexive.

- [3] Write a program to count the number of relations that are transitive on a set X where $|X| = n$. Confirm that $f(4) = 3994$.

```

1 import itertools
2
3 def all_digraphs(n: int):
4     if n <= 0:
5         return []
6
7     # Edge positions to toggle (ordered pairs)
8     positions = []
9     for i in range(n):
10        for j in range(n):
11            positions.append((i, j))
12
13     num_edges = len(positions) # n*(n-1) if no self-loops; n*n if with self-loops
14
15     graphs = []
16     for bits in itertools.product([0, 1], repeat=num_edges):
17         # start with all zeros
18         adj = [[0]*n for _ in range(n)]
19         for (k, (i, j)) in enumerate(positions):
20             adj[i][j] = bits[k]
21         # if self_loops is False, diagonal is already zero by construction
22         graphs.append(adj)
23
24     return graphs
25
26 def is_transitive(r: list[list[int]]) -> bool:

```

```

27     for i in range(4):
28         for j in range(4):
29             for k in range(4):
30                 if r[i][j] and r[j][k]:
31                     if not r[i][k]:
32                         return False
33     return True
34
35 n = 4
36 relations = all_digraphs(n)
37 print(relations[0])
38
39 num_transitive = sum(is_transitive(r) for r in relations)
40 print(num_transitive)

```

4. [2] We say a relation is antittransitive if xRy and yRz implies $\sim(xRz)$. By any means possible determine the number of antittransitive relations on X when $|X| = 5$.

To save you from running the code (takes a couple minutes), the final result is 471552.

```

1 import itertools
2
3 def all_digraphs(n: int):
4     if n <= 0:
5         return []
6
7     # Edge positions to toggle (ordered pairs)
8     positions = []
9     for i in range(n):
10        for j in range(n):
11            positions.append((i, j))
12
13     num_edges = len(positions) # n*(n-1) if no self-loops; n*n if with self-loops
14
15     for bits in itertools.product([0, 1], repeat=num_edges):
16         # start with all zeros
17         adj = [[0]*n for _ in range(n)]
18         for (k, (i, j)) in enumerate(positions):
19             adj[i][j] = bits[k]
20         # if self_loops is False, diagonal is already zero by construction
21         yield adj
22
23
24 def is_anti_transitive(r: list[list[int]]) -> bool:
25     for i in range(4):
26         for j in range(4):
27             for k in range(4):
28                 if r[i][j] and r[j][k]:
29                     if r[i][k]:
30                         return False
31     return True
32
33 relations = all_digraphs(5)
34
35 num_relations = 0
36 num_antittransitive = 0
37 step = 0
38 for r in relations:
39     step += 1
40     if step % 100000 == 0:
41         print(step)
42     num_relations += 1
43     if is_anti_transitive(r):
44         num_antittransitive += 1
45
46
47 print(num_relations, num_antittransitive)

```

Proofs Portfolio

MAT 3100W: Intro to Proofs

Sam Ly

November 3, 2025

1 Introduction

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

2 Mathematical concepts

2.1 Logic, truth tables, and DeMorgan's laws

2.1.1 Logical Statements

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

Example 1. “The sun rose today.” is a **true** logical statement.

Proof. We begin by observing that 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. \square

2.1.2 Truth Tables

Definition 2. Certain logical statements' **truth value** depends on the truth of other statements. For example, “the sun rose today **and** it rained today” requires both statements to be true in order for the overall statement to be true. If the sun rose but it didn't rain, or if the sun hasn't risen but it is raining, the overall statement is false. Thus, to visualize this relationship, it is useful to have a table to lay out the possibilities.

Example 2. $A =$ the sun rose today, $B =$ it rained today.

A	B	$A \wedge B$
T	T	T
T	F	F
F	T	F
F	F	F

2.1.3 DeMorgan's Laws

Definition 3. Logical statements and their combinations have their own form of algebra. One of the fundamental rules are DeMorgan's Laws, which state how to find the complements of conjunctions and disjunctions. *I prefer to use \neg for instead of \sim .*

DeMorgan's Laws:

$$\neg(A \wedge B) = \neg A \vee \neg B$$

$$\neg(A \vee B) = \neg A \wedge \neg B$$

Proof. Refer to direct proofs. □

2.2 Sets

Definition 4. Set: An unordered collection of unique elements.

2.2.1 Unions, intersections, complements, and set differences

2.2.2 Venn diagrams

2.3 Numbers and number systems

Definition 5. Number: values that symbolize quantities. Some quantities may not "make sense" at first glance.

Definition 6. Number system: way of representing numbers. Some are more sophisticated than others.

2.3.1 Parity, divisibility, and modular arithmetic

2.3.2 Rational and irrational numbers

2.3.3 Real numbers, absolute value, and inequalities

2.3.4 Combinatorics: combinations, permutations, and factorials.

2.3.5 Countable sets

2.3.6 Uncountable sets

2.4 Relations and functions

2.4.1 Relations and equivalence relations

2.4.2 Functions

2.4.3 Injections (one-to-one), surjections (onto), and bijections

3 Proof techniques

3.1 Direct Proofs

Definition 7. Direct proof: using fundamental rules of logic to prove a statement.

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

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

Proof. Following from equation 1, we get

$$a = a' + m \times k_1. \quad (3)$$

Similarly, from equation 2, we get

$$b = b' + m \times k_2. \quad (4)$$

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 \times 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, $ab \equiv a'b' \pmod{m}$. \square

3.2 Transformation of conditionals

Definition 8. Transformation of conditionals: using rules of conditional logic to prove conditional statements.

3.2.1 Inverse statements

3.2.2 Converse statements

3.2.3 Contrapositive proofs

3.2.4 Bidirectional ("if and only if" proofs)

3.3 Quantifiers

Definition 9. Quantifier: a logical expression that denotes whether a statement is true for all cases or for specific cases.

3.3.1 Universal quantifiers

3.3.2 Existential quantifiers

3.3.3 Multiply quantified statements

3.4 Existence and uniqueness proofs

Definition 10. Existence and uniqueness proof: a proof that results in us being sure that an element exists with a given property, and that it is the only element that exhibits such property.

3.5 Proof by Induction

Definition 11. Proof by Induction: proof technique used to prove a statement is true for a countably infinite set of discrete elements.

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

Proposition 1. Show that every positive integer is a sum of one or more numbers of the form $2^r 3^s$, 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 $1 = 2^0 3^0$.

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, $n = \sum 2^r 3^s$ where no summand divides another for all nonnegative integers n . \square

Proposition 2. 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

$$\begin{aligned} F_{k+1} &= F_k + F_{k-1} \leq 2.9(1.9^{k-1}) \leq 3.61(1.9^{k-1}) = 1.9^{k+1} \\ &\quad F_{k+1} \leq 1.9^{k+1}. \end{aligned}$$

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

Proposition 3. 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 $f : \mathbb{N} \rightarrow \mathbb{N}$ 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 n th 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

$$\begin{aligned} f(k+1) &= 1 + 2f(k) \\ f(k+1) &= 1 + 2(2^k - 1) \\ f(k+1) &= 2^{k+1} - 1. \end{aligned}$$

Thus, $f(n) = 2^n - 1$. □

3.6 Proof by Contradiction

Definition 12. Proof by contradiction: proof technique that assumes the opposite of our proposition, then showing that this leads to an absurd conclusion, ie. a contradiction. Used as a “last resort” proof technique.

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
 - 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}