1 Disclaimer

The TAs do not know what is on the midterm. The following is our guide for what we believe will be helpful in preparation. Additionally, the example proofs we provide in this review guide may be informal, or stripped to their bare bones. They strive to convey an idea, but are not necessarily paragons of perfect proofs. We suggest looking at the website or the homework solutions for completely polished proofs.

2 Proof Techniques

2.1 Direct Proof

We directly use our statements to imply ($\Rightarrow$) that our conclusion is correct.

Example: Prove the claim that the product of two odd numbers is odd.

2.2 Contradiction

Say we have some proposition $T$ that we are trying to prove. Here is how we can prove it by contradiction:

1. Assume $T$ is not true.
2. Given $T$ is false, use a direct proof to obtain a contradiction.
3. Since $T$ being false leads us to a contradiction, $T$ must be true.

Often $T$ is of the form “If $p$ then $q$.” In this case, assume that $p$ is true and $q$ is false to reach a contradiction. Often, this contradiction will be of the form “If $p$ is true and $q$ is false then $p$ is false. This is a contradiction as $p$ cannot both be true and false.

Example: Prove the claim that if $n^2$ is even, then $n$ is even.
Example: Consider a set $A = \{a_1, ..., a_n\}$ with cardinality $n$.
Consider $f : P(A) \rightarrow \{0, 1\}^n$ where $f(X) = s_1s_2...s_n$ and $s_i = 1$ if $x_i \in X$ and $s_i = 0$ if $x_i \notin X$.
Prove the claim that if $f(X_1) = f(X_2)$ then $X_1 = X_2$.

2.3 Proof by Cases

Example: Prove the claim that there exists $x, y$ irrational such that $x^y$ is rational.

2.4 Counterexample

Counterexamples help us prove that something is not true.
For example, suppose Kristy makes the claim that if $xy$ is rational then $x$ and $y$ are rational.
Kareem can disprove her claim by coming up with a counterexample. For example, if $x = \sqrt{2}$ and $y = \sqrt{2}$, then $xy = 2$, which is rational.
However, you cannot prove a claim by showing one example of it. Kareem has not proven that $x$ and $y$ are irrational, he has just shown that they are not always rational.
For example, the claim “all CS22 students like donuts” can be disproved by finding a student who does not like donuts. Finding this counterexample, however, will not prove that no students like donuts.
Example: Prove the claim that $\mathcal{P}(A \cup B) \neq \mathcal{P}(A) \cup \mathcal{P}(B)$.

2.5 Proof by Element Method

How do you prove that $A = B$? First show that $A \subseteq B$ and then you show that $B \subseteq A$.
If every element in $A$ is also an element in $B$ and every element in $B$ is also an element of $A$, then $A$ must equal $B$. 
To show that $A \subseteq B$ you consider an arbitrary element in $A$ and show it is also in $B$. Example: Prove the claim that $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.

2.6 Bijective Proof

Example provided later. (Put together proofs for injectivity and surjectivity further down in this sheet, and then add conclusion.)

2.7 Bidirectional Proof

If a claim is of the form “$A$ if and only if $B$,” you must prove both “if $A$, then $B$” and “if $B$, then $A$”

2.8 Inductive Proof

More detail later.

3 Logic

Here’s information about logic.

3.1 Preliminary Definitions

1. A propositional formula is a condensed representation of a truth table using logical operators and variables. We call a propositional formula a proposition for short.

2. The term logical expression is often used synonymously with the word proposition.

3. Two propositions are logically equivalent when they represent the same truth table. We can prove propositions are logically equivalent by either comparing their truth tables or using logical rewrite rules. A full list of the rules you can use is on our course website.
4. A valid proposition is one that evaluates to true on any choice of inputs; it is true no matter what. It is also sometimes called a tautology. The classic example of a valid proposition is $b$ OR NOT $b$ (thanks, Shakespeare).

5. A proposition is satisfiable if it evaluates to true on some choice of inputs; that is, there is some assignment of the input variables to true and false that makes the proposition true.

6. A proposition is unsatisfiable if it is false on any choice of inputs; it is false no matter what. It is also sometimes called a contradiction. The classic example of an unsatisfiable proposition is $p$ AND NOT $p$.

Let’s now review the interpretation of each of the following logical operators:

<table>
<thead>
<tr>
<th>$P$</th>
<th>$Q$</th>
<th>NOT $P$</th>
<th>$P$ AND $Q$</th>
<th>$P$ OR $Q$</th>
<th>$P$ XOR $Q$</th>
<th>$P$ IMPLIES $Q$</th>
<th>$P$ IFF $Q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>T</td>
</tr>
</tbody>
</table>

3.2 Implication

In the formula $P$ IMPLIES $Q$, we call $P$ the hypothesis and $Q$ the conclusion. $P$ IMPLIES $Q$ is logically equivalent to NOT $P$ OR $Q$. In words, this means that for $P$ IMPLIES $Q$ to be true, $Q$ must be true or $P$ must be false.

This choice can seem a little strange at first. Why is $P$ IMPLIES $Q$ true when $P$ is false? Consider the following statement: “If it is raining, I will bring my umbrella.” Here are the events that could possibly occur.

- It rains, and I bring my umbrella. That seems fine. The statement is consistent with the situation.
- It rains, and I don’t bring my umbrella. The statement does not fit with the situation.
- It doesn’t rain, and I bring my umbrella. This situation doesn’t seem to directly conflict with the statement. After all, what if I brought my umbrella to block the sun instead? As a result, we say the statement is still consistent with the situation.
- It doesn’t rain, and I don’t bring my umbrella. The statement seems consistent with this situation, too.

The only scenario that where the statement doesn’t fit is the second, which is why $P$ IMPLIES $Q$ is only false when $P$ is true and $Q$ is false.
• \( \text{NOT } Q \text{ IMPLIES NOT } P \) is called the contrapositive of \( P \text{ IMPLIES } Q \) and is logically equivalent. As a result, we have a useful proof technique: to prove the statement "if \( p \), then \( q \)" we can instead prove "if not \( q \), then not \( p \)."

• \( Q \text{ IMPLIES } P \) is called the converse of \( P \text{ IMPLIES } Q \). It is not logically equivalent to \( P \Rightarrow Q \). If both a statement and its converse are true, then the biconditional \( P \text{ IFF } Q \) is true.

### 3.3 Normal Forms

A literal is a variable or its negation.

We say a proposition is in **DNF** (disjunctive normal form) when it is the disjunction (clauses ORed together) of conjuctions (literals ANDed together).

We say a proposition is in **CNF** (conjunctive normal form) when it is the conjuction (clauses ANDed together) of disjuctions (literals ORed together).

Here's a truth table, and propositions in DNF and CNF that represent it:

| \( P \) | \( Q \) | \( R \) | ?
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>T</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>T</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>T</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
</tbody>
</table>

DNF: \((P \text{ AND } Q \text{ AND NOT } R) \text{ OR } (P \text{ AND NOT } Q \text{ AND NOT } R)\)

OR \((\text{NOT } P \text{ AND NOT } Q \text{ AND } R) \text{ OR } (\text{NOT } P \text{ AND NOT } Q \text{ AND NOT } R)\)

CNF: \((\text{NOT } P \text{ OR NOT } Q \text{ OR NOT } R) \text{ AND } (\text{NOT } P \text{ OR } Q \text{ OR NOT } R)\)

AND \((P \text{ OR NOT } Q \text{ OR NOT } R) \text{ AND } (P \text{ OR NOT } Q \text{ OR } R)\)

If we have an arbitrary truth table, here are two ways we can think about describing it:

- Listing the true rows.
- Listing the false rows.

Since every row must be either true or false, both of these ways will uniquely describe our truth table.

These two ways correspond to DNF and CNF, respectively. To write a proposition in DNF, we can think about it like this: we find all rows where our proposition should evaluate to true, and we say that we must be in one of those rows. On the other hand,
to write a proposition in CNF, we find all rows where our proposition should evaluate
to false, and say we are not in any of those rows.

For DNF, we AND the true variables and negations of the false variables (to be in
the row, the inputs must exactly correspond to the row). For CNF, we OR the false
variables and the negations of the true variables (to not be in the row, we just need at
least one variable to be different).

In this way, we can represent any truth table in CNF or DNF. We can also rewrite any
logical expression to be in CNF or DNF.

3.4 Circuits

Circuits are another way to represent truth tables. Circuits can have multiple outputs,
unlike propositions; that is, circuits can represent more than one truth table. The
number of outputs they have corresponds to the number of truth tables they represent.

Here are what the different gates look like in circuit notation.

We can chain them together to make circuits! For instance, this circuit represents
propositions \(x = p \text{ AND } (q \text{ AND } r)\) and \(y = (p \text{ OR } q) \text{ OR NOT } r\).
4 Sets and Notation

A set is a collection of objects without order or repetition.

4.1 Membership vs. Subsets

If an object \( s \) is a member of a set \( S \), we say \( s \in S \). If a set \( T \) is a subset of a set \( S \), we write \( T \subseteq S \). This means that every member of \( T \) is also a member of \( S \).

a. \( A \) is any set. Which of the following is always true?
   i. \( A \subseteq A \)
   ii. \( \{\} \subseteq A \)
   iii. \( \{\} \in A \)

b. \( A \) is any set and \( \mathcal{P}(A) \) is the set of all subsets of \( A \). Which of the following is always true?
   i. \( A \in \mathcal{P}(A) \)
   ii. \( A \subseteq \mathcal{P}(A) \)
   iii. \( \emptyset \in \mathcal{P}(A) \)
   iv. \( \emptyset \subseteq \mathcal{P}(A) \)
   v. \( \{A, \emptyset\} \subseteq \mathcal{P}(A) \)

c. \( S \) is the set of students in CS22. \( B \) is the set of students at Brown. Duncan is a student in CS22. Which of the following is always true?
   i. \( S \subseteq B \)
   ii. Duncan \( \subseteq S \)
   iii. Duncan \( \in S \)
   iv. \( \{\text{Duncan}\} \subseteq B \)

4.2 Set Operations

The union \( A \cup B \) of two sets \( A \) and \( B \) is the set of all elements that are in \( A \) or \( B \).

The intersection \( A \cap B \) of two sets \( A \) and \( B \) is the set of all elements that are in \( A \) and \( B \).

The set difference \( B - A \) of two sets \( A \) and \( B \) is the set of all elements that are in \( B \), but that are not in \( A \).
The complement $\overline{A}$ of a set $A$ is the set of all elements that are not in $A$ (where “all elements” refers to all elements in some universal set $U$.)

The cardinality $|A|$ of a set $A$ is the number of elements of $A$. Remember that sets have no duplicates!

### 4.3 Power Sets

The *power set* of a set $S$, denoted $\mathcal{P}(S)$ is the set of all subsets of $S$. The power set of $S$ has cardinality $2^{|S|}$. We proved this last result by noticing that there are the same number of subsets of a set of size $n$ as there are binary strings of length $n$ (see the sample bijective proof on the website).

### 4.4 Product

The product of two sets $A$ and $B$, denoted $A \times B$, is the set of all ordered pairs $(a, b)$ for $a \in A$, $b \in B$. The product of a single set, $A$, is the set of all ordered pairs $(a, a)$ where $a \in A$.

### 5 Relations

#### 5.1 Relation on $A \times B$ vs. Relation on $A$

A *relation* $R$ on the sets $A$ and $B$ is a subset of the Cartesian product $A \times B$. A relation $R$ on the set $A$ is a subset of the Cartesian product $A \times A$.

Always remember to specify the set(s) on which the relation is defined!

#### 5.2 Notation

$aRb$ and $(a, b) \in R$ are both compact ways of saying the same thing: $a$ is related to $b$ in $R$.

Remember that a relation is a set of ordered pairs, not a description of the way elements are linked. For example, the following is a relation on $\mathbb{Z}$:

$$R = \{(x, y) \mid x \leq y\}.$$  

However, “$\leq$” is not a relation.

#### 5.3 Reflexivity

A relation $R$ on $A$ is *reflexive* if for all $a \in A$, $(a, a) \in R$. In other words, a relation is reflexive if *every element* in the set $A$ is related to itself in $R$. This is why it’s important
to specify a set when talking about a relation: you can’t tell if a relation is reflexive if you don’t know which elements have to be related to themselves (and every element must be!)

5.4 Symmetry and Transitivity

A relation $R$ on $A$ is **symmetric** if for all $a, b \in A$, the following holds: if $(a, b) \in R$, then $(b, a) \in R$.

A relation $R$ on $A$ is **transitive** if for all $a, b, c \in A$, the following holds: if $(a, b) \in R$ and $(b, c) \in R$, then $(a, c) \in R$. Remember that $a$, $b$, and $c$ do not need to be different elements.

It’s important to note that the definitions of symmetry and transitivity are phrased as if-then statements. A relation is symmetric/transitive unless it violates the appropriate if-then condition. To violate the condition, you must simultaneously satisfy the if-clause, and violate the then-clause.

Consider the following example of a relation that is not transitive: the order pairs $(1, 2)$ and $(2, 1)$ are in the relation (this satisfies the if-clause of the transitivity definition) but there is no pair $(1, 1)$ in the relation (this violates the then-clause.) As another illustrative example: any empty relation is both symmetric and transitive, as there are no ordered pairs in the empty relation to satisfy the if-clause of either definition.

5.5 Equivalence Relation

An **equivalence relation** is a relation that is reflexive, symmetric, and transitive.

5.6 Equivalence Classes

Let $R$ be an equivalence relation on $A$. Then the **equivalence class** of $a \in A$ is defined as

$$[a]_R := \{x \mid x \in A, (x, a) \in R\}.$$ 

Note that $a$ is not unique (unless it is the only element in its equivalence class.) Rather, any element in the same equivalent class can serve equally well as the representative for the class.

An equivalence relation splits a set into equivalences classes. In other words, it forms a partition of the set.

A **partition** of a set $A$ is a collection of nonempty subsets $B_1, \ldots, B_k$ of $A$ such that

1. $B_1 \cup \cdots \cup B_k = A$, and
2. $B_i \cap B_j = \emptyset \forall i, j$ where $i \neq j$. 


5.7 Examples

Consider the set $B$ of all students at Brown. For each of the following relations on $B$, state if they are reflexive, symmetric, or transitive. If they are an equivalence relation then list the equivalence classes.

i. Two students are related if they are the same age (e.g. 21).
ii. $s_1$ and $s_2$ are students and $(s_1, s_2) \in R$ if $s_1$ is younger than $s_2$.
iii. Two students are related if they are studying anthropology.
iv. Two students are related if they go to Brown.

Let $A = \{1, 2, 3\}$. Consider the following relations on $\mathcal{P}(A)$. State if they are reflexive, symmetric, or transitive. If they are an equivalence relation then list the equivalence classes.

i. $(S_1, S_2) \in R$ if $|S_1| = |S_2|$.
ii. $(S_1, S_2) \in R$ if $S_1 \subseteq S_2$.
iii. $(S_1, S_2) \in R$ if $S_1$ and $S_2$ share an element.

6 Functions

6.1 Formal Definition

A function $f : A \rightarrow B$ is a relation on $A$ and $B$ with the following property: for every $a \in A$ there exists exactly one pair $(a, b)$ in the relation, where $b \in B$.

We call $A$ the domain and $B$ the codomain.

It’s important to note that a function is characterized not only by the “rule” that maps inputs to outputs, but also by the domain and codomain.

Additionally, we call the set of all $b \in B$ such that there exists $a \in A$ where $f(a) = b$ the image of $f$. In other words, the image is the set of all elements mapped to by $f$.

6.2 Injectivity

A function is injective if for all $b \in B$, there exists at most one $a \in A$ such that $f(a) = b$. In other words, no two distinct elements map to the same thing! Another way to think about this: if you give me an element in the image of the function, I can tell you without
a doubt which element mapped to it. Why? Because there won’t be more than one element that maps to it.

If a function \( f : A \to B \) is injective, we know that \( |A| \leq |B| \). This is because every element in \( A \) needs some unmatched element in \( B \), so \( B \) needs to have at least as many elements as \( A \)!

There are two ways to prove that a function is injective:

1. Consider two arbitrary distinct elements in the domain. Show that they must map to distinct outputs.

2. Consider two equal elements in the image of \( f \) (say, \( f(a) \) and \( f(b) \)). Show that \( a = b \).

### 6.3 Surjectivity

A function is surjective if for all \( b \in B \), there exists at least one \( a \in A \) such that \( f(a) = b \). In other words, no element in the codomain gets left behind: there is always some element that maps to it. Equivalently, a function is surjective if the image of the function is the entire codomain.

If a function \( f : A \to B \) is surjective, we know that \( |A| \geq |B| \). This is because every element in \( B \) needs some element in \( A \) to map to it, so \( A \) needs to have at least as many elements as \( B \).

To prove that a function is surjective, consider an arbitrary element in the codomain, and construct the specific element in the domain that maps to it.
6.4 Bijectivity

A bijection is a function that is both injective and surjective. Thus, to prove that a function is a bijection, prove that it is injective and surjective.

If we combine our results from injectivity and surjectivity, we know that the cardinality of the domain must be less than or equal to that of the codomain (by injectivity), and that the cardinality of the domain must be greater than or equal to that of the domain (by surjectivity.) Thus, the cardinalities of the two sets must be equal. This is a powerful result:

There exists a bijection between two sets if and only if they have equal cardinality.

Thus, to prove that the sizes of two sets are equal, it suffices to prove that there exists a bijection between them.

6.5 Intuition and Examples
For each of the following, state if it is a function, injections, surjection, or neither.

(a) \( f : \mathbb{Z} \rightarrow \mathbb{Z} \) where \( f(x) = x^2 \)

(b) \( f : \mathbb{Z}^+ \rightarrow \mathbb{Z}^+ \) where \( f(x) = x^2 \). \( \mathbb{Z}^+ \) denotes the positive integers.

(c) \( f : \mathbb{Z} \rightarrow \mathbb{Z} \) where \( f(x) = \sqrt{x} \).

(d) \( f : \) First Year Students at Brown \( \rightarrow \) First Year Dorms at Brown where \( f(\text{student}) = \) the dorm that the student lives in.

(e) \( f : \) Students at Brown \( \rightarrow \) Banner IDs of current Students where \( f(\text{student}) = \) the banner ID of student.

(f) \( f : \) People in the World \( \rightarrow \) \( \{0, 1\} \) where \( f(\text{person}) = 1 \) if they are Prof. Littman and 0 otherwise.

(g) \( f : \) Library at Brown \( \rightarrow \) \( \mathbb{Z} \) where \( f(\text{Library}) = \) number of books in the library.

(h) \( f : S \rightarrow \mathcal{P}(S) \) where \( f(S) = \{S\} \).

(i) \( f : \mathcal{P}\{\{1, 2, 4\}\} \rightarrow \{0, 1, 2, 3\} \) where \( f(X) = |X| \).

### 7 Induction

#### 7.1 Example 1: Template and Weak Induction

*Idea:* If you are stuck on an induction problem on the exam, start by writing out the inductive hypothesis and the structure of the proof. You will receive partial credit for this and it will also help you think of how to proceed.

*Idea:* Often the inductive step is a direct proof using the inductive hypothesis. This is not always the case, sometimes you might have to use different cases or even contradiction.

We will first provide a review of the template for an inductive proof and provide an example.

For example, say we are trying to prove that \( \sum_{i=0}^{n} i = \frac{n(n+1)}{2} \) is true for all \( n \in \mathbb{N} \).

1. Define the predicate \( P(n) \).

   Let \( P(n) \) be the predicate that \( \sum_{i=0}^{n} i = \frac{n(n+1)}{2} \).

2. Show that the base case is true.

   We will first show \( P(0) \) is true. \( \sum_{i=0}^{0} i = 0 \) and \( \frac{0(0+1)}{2} = 0 \) so they are equal as needed.
3. Assume the inductive hypothesis is true. If you are using standard induction then you will assume \( P(k) \) is true for some integer \( k \). If you are using strong induction then you will assume \( P(i) \) is true for all \( i \leq k \). Either way, you should specify that \( k \) is some integer greater than or equal to your greatest base case.

Assume \( P(k) \) is true for some arbitrary integer \( k \geq 0 \).

4. Show that \( P(k + 1) \) is true given the inductive hypothesis.

We will now show that \( \sum_{i=0}^{k+1} i = \frac{(k+1)(k+2)}{2} \).

We know that \( \sum_{i=0}^{k+1} i = \left( \sum_{i=0}^{k} i \right) + (k + 1) \).

By our inductive hypothesis \( \sum_{i=0}^{k} i = \frac{k(k+1)}{2} \).

Therefore

\[
\sum_{i=0}^{k+1} i = \left( \sum_{i=0}^{k} i \right) + (k + 1) \\
= \frac{k(k+1)}{2} + (k + 1) \\
= \frac{k(k+1) + 2(k+1)}{2} \\
= \frac{(k+1)(k+2)}{2}
\]

as needed.

5. Conclude the proof.

Therefore, as \( P(0) \) is true and \( P(k) \) implies \( P(k + 1) \) for all \( k \in \mathbb{Z} \), \( k \geq 0 \), \( P(n) \) is true for all nonnegative integers \( n \).

7.2 Example 2: Strong Induction

Example: Define the sequence \( S \) as follows: \( S_1 = 1 \), \( S_2 = 3 \), \( S_n = S_{n-1} \ast S_{n-2} \) for integers \( n \geq 2 \). Prove that \( S_n \) is odd for all positive integers \( n \).