Introduction to Discrete Mathematics

Dr. Mark Fitch

December 2, 2014
# Contents

1 Basics 5
  1.1 Sets 5
  1.2 Set Operations 6
  1.3 Combinatorics: First Counts 7
    1.3.1 Permutations: First Time 7

2 Logic 9
  2.1 Formal Logic 9
  2.2 Circuits 11
  2.3 Predicate Logic 11
  2.4 Quantifiers 11
  2.5 Negation 11

3 Applications of Logic 13
  3.1 Proof 13
    3.1.1 Direct Proof 13
    3.1.2 False Statements 13
    3.1.3 Vacuous Truth 14
    3.1.4 Existence 14
    3.1.5 Uniqueness 14
  3.2 Boolean Algebra 15
    3.2.1 Duality 16
    3.2.2 Representation 16

4 More Basics 19
  4.1 Modulo Arithmetic 19
  4.2 Combinatorics: Second Counts 19
    4.2.1 Combinations 20

5 Equivalence Relations 21
  5.1 Relations 21
  5.2 Equivalence Relations 23
  5.3 Equivalence Classes 23

6 Partially Ordered Sets 25
  6.1 Definition 25
  6.2 Representation 25
  6.3 Properties 26
  6.4 Lattice 26

7 More Proofs 27
  7.1 Contradiction 27
  7.2 Functions 27
8 Graph Theory
  8.1 Definition ................................................................. 31
  8.2 Graph Properties ....................................................... 32
  8.3 Isomorphism .............................................................. 35
  8.4 Paths ................................................................. 35
  8.5 Connected .......................................................... 36
  8.6 Cycles .............................................................. 37
  8.7 Trees ............................................................ 38

9 More Enumeration ................................................. 39
  9.1 Inclusion/Exclusion .................................................. 39
  9.2 Recursion Relations ................................................... 40
  9.3 Induction .......................................................... 41

A Appendix ................................................................. 43
  A.1 UA Database .......................................................... 43
Chapter 1

Basics

1.1 Sets

The first structure is the set. Essentially a set is a description of what is included and what is excluded.

Problem 1 Determine whether or not you are in the following sets.

1. UAA students
2. Computer Science majors
3. millionaires
4. musicians

In mathematics concepts must be “well defined.” This means there are no ambiguities. For sets this means that it must be possible to determine whether every object is in a set or not.

Note this does not mean that any person necessarily knows the answer, rather that some means exists. For example every number is prime or it is not. However, no person knows or can list all the primes.

Problem 2 Are all of the sets above well defined?

Problem 3 Given that sets indicate what is included and excluded do the following descriptions of sets make sense?

1. \{ green, gold, gold, green \}
2. \{1, 2, 3, 4, 5, \ldots \}
3. \{0, 0, 1, 0, 1, 0, 1\}
4. all even numbers

Formally,

Definition 1 (Set) A collection of objects is a set if and only if the collection is unordered.

Sets are often described by listing all the elements as in \{1, 2, 3, 4, 5, \ldots \} or by specifying a pattern as in \{n|n = 2k for some integer k\}. The latter is read “the set of all n such that n is the product of 2 and some integer.” Alternately the latter can be written \{n : n = 2k for some integer k\}. The | or : denote the beginning of the pattern’s description.

Objects in a set are called members and are described as being ‘in’ the set. This is denoted \(a \in A\) where \(a\) is the member and \(A\) is some set.

Definition 2 (Subset) A set \(A\) is a subset of a set \(B\), denoted \(A \subseteq B\), if and only if \(a \in A\) implies \(a \in B\).
Problem 4 Determine if the first set is a subset of the second set.

1. even numbers, all integers
2. vowels, letters
3. colors, pastels
4. chairs, people

1.2 Set Operations

Just as there are arithmetic operations on numbers, there are set operations on sets.

Definition 3 (Union) The set \( C \) is the union of the sets \( A \) and \( B \), denoted \( A \cup B \), if and only if \( C = \{x| x \in A \text{ or } x \in B\} \).

Definition 4 (Intersection) The set \( C \) is the intersection of the sets \( A \) and \( B \), denoted \( A \cap B \), if and only if \( C = \{x| x \in A \text{ and } x \in B\} \).

Definition 5 (Difference) The set \( C \) is the difference between the sets \( A \) and \( B \), denoted \( A - B \), if and only if \( C = \{x| x \in A \text{ but } x \notin B\} \).

In many circumstance there is a universal set that is part of the context for a problem. For example the set of all integers may be the universal set for discussion of even and odd numbers.

Definition 6 (Complement) The set \( C \) is the complement of the set \( A \) with respect to the universal set \( U \), denoted \( \neg A \) or \( \overline{A} \), if and only if \( C = U - A \).

![Set Operations Diagram]

Problem 5 Identify the following in the diagram above.

1. \( A \cup B \)
2. \( A \cap B \)
3. \( A - B \)
4. \( B - A \)
5. \( \neg A \)
6. \( \neg B \)

Problem 6 Identify the following for the sets \( A = \{n| n = 6k \text{ for some integer } k\} \) and \( B = \{n| n = 10k \text{ for some integer } k\} \). The universal set is all integers.
1.3. COMBINATORICS: FIRST COUNTS

1. $A \cup B$
2. $A \cap B$
3. $A - B$
4. $B - A$
5. $\neg A$
6. $\neg B$

Definition 7 (Power Set) The set $P$ is the power set of a set $A$, denoted $\mathcal{P}(A)$ or $2^A$, if and only if $P$ is the set of all subsets of $A$.

For example if $A = \{0, 1\}$ then $\mathcal{P}(A) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$.

Definition 8 (Cartesian Product) The set $C$ is the Cartesian product of the sets $A$ and $B$, denoted $A \times B$, if and only if $C = \{(a, b) | a \in A \text{ and } b \in B\}$.

For example if $A = \{0, 1\}$ and $B = \{a, b\}$ then $A \times B = \{(0, a), (0, b), (1, a), (1, b)\}$.

Problem 7 Calculate the following for $A = \{0, 1, 2\}$ and $B = \{0, 1\}$.
1. $\mathcal{P}(A)$
2. $A \times B$
3. $B \times A$

1.3 Combinatorics: First Counts

Combinatorics is the mathematics of counting.

Definition 9 (Word) A collection of objects is called a word if and only if it is ordered. The set of objects is called the alphabet.

A few words from the alphabet $\{a, b, c\}$ are the following: $c$, $abc$, $bc$, $cab$, $ccb$, $aaa$.

Problem 8 Generate a list of all possible words of length two from the alphabet $\{0, 1\}$.

Problem 9 How many words of length three are possible from the alphabet $\{0, 1\}$?

Problem 10 How many words of length three are possible from the alphabet $\{0, 1, 2\}$?

1.3.1 Permutations: First Time

A permutation counts the number of ways to permute (rearrange) the characters in a word. Some of the permutations of the word ‘abc’ are the following: $abc$, $bac$, $cab$.

Problem 11 Write all permutations of the word ‘math’.

Problem 12 How many permutations are there of the word ‘heat’.

Problem 13 How many permutations are there of the word ‘great’.
Chapter 2

Logic

2.1 Formal Logic

The previous chapter used words like ‘and’ and ‘or’ and required deciding what is true. This chapter presents a formal approach to these topics and ends by applying it to program and circuit logic.

Definition 10 (Statement) An expression is a statement if and only if it is either true or false.

The following are statements. ‘The sky is blue.’ ‘George Washington was the first president of the United States.’ The following are not statements. ‘Hello.’ ‘Study hard.’ ‘Is that true?’ For convenience letters, such as A and B, are used to refer to statements. 0 represents false and 1 represents true.

Statements can be modified and combined. Figure 2.1 gives the definitions for some of these logic operations.

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>A and B</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>A and B</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>if A, then B</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Figure 2.1: Definition of Logic Operations

These diagrams are called truth tables. For convenience the following symbols are used for these operations.

- not  ¬
- and  ∧
- or   ∨
- if   →

As with arithmetic operations there is an order of operations. The tables above list the operators in first to last order.

Problem 14 Complete the following truth tables.

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>A → B</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

1.
CHAPTER 2. LOGIC

Problem 15 Complete the following truth table.

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>\neg B</th>
<th>A \land B</th>
<th>\neg (A \land B)</th>
<th>\neg A</th>
<th>\neg B</th>
<th>\neg (A \lor B)</th>
<th>\neg (A \land \neg B)</th>
<th>\neg (A \lor \neg B)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td></td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>1</td>
<td></td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td></td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td></td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td></td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Two, possibly compound, statements A and B are considered to be equivalent if they have the same truth value for all inputs. This is denoted $A \leftrightarrow B$. Figure 2.2 provides truth tables that show two pairs of equivalent statements known as DeMorgan’s Laws.

Problem 16 Are any of the statements in Problem 14 equivalent?
2.2 Circuits

Digital circuits are built by combining large numbers of pieces, called gates. Gates take one or two electrical inputs which are either low (0) or high (1) current and output a single current. The gates act like negation, and, and or. Figure 2.3 shows the symbols that are used on diagrams for these three gates.

![Figure 2.3: Symbols for Circuits](image)

An example of combining gates to produce a more complicated circuit is shown in the following circuit for ‘if.’

![Circuit Diagram](image)

**Problem 17** Draw the circuit diagram that accepts three inputs $a, b, c$ and outputs $a \land (\neg b \lor c)$.

2.3 Predicate Logic

In order to efficiently communicate logic statements we use predicates. These are simply functions with a codomain of ‘true’ and ‘false.’ For example $R(x) = x$ is red. Thus $R(\text{stop sign}) = \text{true}$ and $R(\text{Seawolf logo}) = \text{false}$. More complicated statements can be expressed as well. The following example converts the statement $n$ is even and positive into symbols using predicates.

$E(n) \equiv n$ is even.
$P(n) \equiv n > 0.$
$E(n) \land P(n).$

2.4 Quantifiers

For predicates we often ask the questions, “does any object satisfy the predicate” and “what is true of all objects that satisfy the predicate.” These two questions add quantifiers to logic. Consider the following predicates:

$E(n)$ is $n$ is even
$P(n)$ is $n$ is prime
$Q(n)$ is $n$ is a multiple of 4.

We can assert “there exist $n$ such that $E(n) \land Q(n)$.” We can also assert “if $Q(n)$, then $E(n)$.”

The first question, “does any object satisfy the predicate,” is the existential question. The symbol $\exists$ is used for “there exists.” The first example above can be written as $\exists n \ni E(n) \land P(n)$.

The second question “what is true of all objects that satisfy the predicate,” is the universal statement. The symbol $\forall$ is used for “for all.” The second example above can be written as $\forall n Q(n) \rightarrow E(n)$.

**Problem 18** Write the following statement using predicates and quantifiers. “All computer science majors must take Introduction to Discrete Mathematics and Data Structures and Algorithms.”

2.5 Negation

In order to simplify logic statements we often desire to change a negative statement into a positive statement. Consider the following example.
It is not true that Guido owns a sail boat and has either a type rating for the Cessna Citation X or likes to cook. What does this tell us about Guido. To determine this predicate notation will help.

\( S(x) \) \( x \) owns a sail boat.
\( C(x) \) \( x \) has a type rating for the Cessna Citation X.
\( K(x) \) \( x \) likes to cook.

The original statement can now be written as

\[ \neg (S(\text{Guido}) \land (C(\text{Guido}) \lor K(\text{Guido}))) \]

DeMorgan’s Law changes this to

\[ \neg S(\text{Guido}) \lor \neg (C(\text{Guido}) \lor K(\text{Guido})) \]

The other DeMorgan’s Law changes this to

\[ \neg S(\text{Guido}) \lor (\neg C(\text{Guido}) \land \neg K(\text{Guido})). \]

Returning this to English gives us

Either Guido does not own a sailboat, or he does not have the Cessna Citation X type rating and he does not like to cook.

In addition to DeMorgan’s Laws the negations of the two quantifiers are needed.

<table>
<thead>
<tr>
<th>Name</th>
<th>Hair</th>
<th>Eye</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guido</td>
<td>Brown</td>
<td>Brown</td>
</tr>
<tr>
<td>Wolfgang</td>
<td>Red</td>
<td>Brown</td>
</tr>
<tr>
<td>Ludwig</td>
<td>Brown</td>
<td>Hazel</td>
</tr>
<tr>
<td>Franz</td>
<td>Brown</td>
<td>Brown</td>
</tr>
<tr>
<td>Maria</td>
<td>Gray</td>
<td>Brown</td>
</tr>
</tbody>
</table>

Problem 19 How would you show that the statement “All of the five friends have brown hair” is false?

Problem 20 How would you show that the statement “Some of the five friends have blue eyes” is false?

Problem 21 What is the negation of the following statement. “All Apple fanboy’s own an iPad.”

Problem 22 What is the negation of the following statement. “Some chemist likes to cook.”
Chapter 3
Applications of Logic

3.1 Proof

The previous section discussed statements that were true or false. Now we must consider how we demonstrate that a statement is either true or false. There are at least two reasons to do this. First, we need a means to be confident that the statements we make and use are correct. Second, we need a means to communicate our work to each other. For further discussion of views of truth and communication study epistemology and rhetoric

Like any communication there is no algorithm that produces a good result all the time. Figuring out how to prove statements is an art. However, many statements provide hints for a good approach and there are best practices for expressing proofs.

3.1.1 Direct Proof

It is possible to prove a statement is true by direct demonstration. Consider the following example.

Definition 11 (Solution of an Equation) A value $x$ is a solution to an equation if and only if substitution of the value $x$ into the equation results in a true statement.

Statement: 5 is a solution of $3x - 11 = 4$.

Proof: Note $3(5) = 15$, $15 - 11 = 4$, so $3(5) - 11 = 4$ or $4 = 4$ which is a true statement.

More frequently we are trying to prove a conditional statement is true. Thus there are no specific values to use in a calculation. However, proofs for many problems can be written by starting with the condition and applying known, true statements to arrive at the conclusion. This is called a direct proof. Consider the following example.

$A \cap B \subset A$.

Proof: Let $x \in A \cap B$. By definition of intersection, $x \in A$ and $x \in B$. Thus $x \in A$. Because $x \in A \cap B$ implies $x \in A$ $A \cap B \subset A$ by definition of subset.

Problem 23 Prove that $A \subset A \cup B$.

Problem 24 Prove that $A - B \subset A$.

Problem 25 Prove $B - (A - B) = B$.

3.1.2 False Statements

Proving a statement is false is often easy. Consider the following example.

Statement: 7 is a solution of $3x - 11 = 4$.

This is false. Consider $3(7) = 21$ and $21 - 11 = 10$. However, $10 \neq 4$.

Proving conditional statements are false can sometimes be easy as well.

Problem 26 Review the truth table for ‘if.’ Which combination of truth values makes if $A$ then $B$ false?
Consider the following example.

\[ A - B \subset B. \]

This statement is false. Consider \( A = \{1,2,3,4,5,6\} \) and \( B = \{2,4,6\} \). Thus \( A - B = \{1,3,5\} \). Note 1 \( \notin B \). Thus \( A - B \notin B. \)

**Problem 27** Show that the following statement is false. \( A - B = B - A. \)

### 3.1.3 Vacuous Truth

Direct proofs show that \( A \rightarrow B \) is true by starting with \( A \) true and using true statements to arrive at \( B \) true. Proving \( A \rightarrow B \) is false requires finding a case where \( A \) is true but \( B \) is false. These cover two of the four entries in the truth table for ‘if.’ The other two entries begin with \( A \) is false. Note that the conditional is true for both of these cases. Consider the following that illustrate why these cases are true.

Suppose Guido runs for president promising that ‘If I am elected president, Mount McKinley will be officially renamed Denali.’

**Problem 28** If Guido is not elected, but he manages to lobby the U.S. Congress to make this name change, has he upheld his promise?

**Problem 29** If Guido is not elected and the legislative delegation from Ohio preserves McKinley as the name of the mountain, has Guido upheld his promise?

**Problem 30** Prove that the following legend is true. Wise old elders claim that when the sun rises on January 1st in Barrow, AK the polar bears turn green.

### 3.1.4 Existence

Proving a ‘for all’ statement is simply proving a conditional statement, because the universal quantifier is equivalent to a conditional. However, existence proofs are different, and they are often easier.

**Problem 31** What do you think would be a good method to prove that \( 7x - 13 = 99 \) has a real number solution?

**Problem 32** There is an integer whose only non-negative, integer divisor is 1.

**Problem 33** There is a set that is a subset of every set.

Note not all existence proofs are this simple. Not all are direct proofs. Some proofs demonstrate existence without any hint at how to find that which exists. For example it is possible to demonstrate that a sequence converges to some real value without knowing what that value is. For details check any calculus textbook.

### 3.1.5 Uniqueness

In some cases we can prove not only that something exists, but also that there is only one object meeting all the conditions. Consider the following example.

For any real number \( a \) there exists exactly one real number \( b \) such that \( a + b = 0. \)

**Proof: Existence**

Note \( a + (\neg a) = 0. \) Thus \( b = \neg a \) is a solution by definition of negative real numbers.

**Proof: Uniqueness**

Suppose there exist \( b, c \) such that \( a + b = 0 \) and \( a + c = 0. \) Then

\[
\begin{align*}
a + b &= a + c, \\
\neg a + a + b &= \neg a + a + \text{cxiom: like added to like is still equal} \\
&= b = c.
\end{align*}
\]

Thus the real number \( b \) is unique.
3.2. BOOLEAN ALGEBRA

Note the following is not a proof of uniqueness. Suppose

\[
\begin{align*}
    a + b &= 0, \\
    -a + a + b &= -a + 0, \\
    b &= -a.
\end{align*}
\]

Thus \( b \) is unique because adding \(-a\) (or any other number) generates only one solution.

Unfortunately this assumes that there was no other number, say \( c \) such that \( c + a + b = c + 0 \) gives \( b = c \). Actually this is the purpose of this proof.

3.2 Boolean Algebra

It is possible to process logic concepts using arithmetic and algebra concepts. To do so the following arithmetic definitions are needed. The first table defines addition the second defines multiplication and the third defines complement.

<table>
<thead>
<tr>
<th>+</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>·</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

\( \overline{0} = 1 \)
\( \overline{1} = 0 \)

**Problem 34** Compare these three operations to the logical operations \( \neg, \lor, \text{ and } \land \).

Functions can be defined using boolean algebra as well. Consider the following examples.

<table>
<thead>
<tr>
<th>( x )</th>
<th>( y )</th>
<th>( f_1(x,y) = x + y )</th>
<th>( f_2(x,y) = xy )</th>
<th>( f_3(x,y) = x + x )</th>
<th>( f_4(x,y) = \overline{x} + y )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 0</td>
<td>0 1</td>
<td>0 1</td>
<td>0 0</td>
<td>0 1</td>
<td>1 1</td>
</tr>
<tr>
<td>0 1</td>
<td>1 0</td>
<td>1 0</td>
<td>0 0</td>
<td>1 0</td>
<td>1 0</td>
</tr>
<tr>
<td>1 0</td>
<td>1 1</td>
<td>1 1</td>
<td>1 0</td>
<td>1 1</td>
<td>1 1</td>
</tr>
</tbody>
</table>

**Problem 35** Evaluate the following boolean functions.

<table>
<thead>
<tr>
<th>( x )</th>
<th>( y )</th>
<th>( f_1(x,y) = 1 + x )</th>
<th>( f_2(x,y) = \overline{xy} )</th>
<th>( f_3(x,y) = \overline{x} + \overline{y} )</th>
<th>( f_4(x,y) = xy + y )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 0</td>
<td>0 1</td>
<td>0 1</td>
<td>0 0</td>
<td>0 1</td>
<td>1 1</td>
</tr>
<tr>
<td>0 1</td>
<td>1 0</td>
<td>1 0</td>
<td>0 0</td>
<td>1 0</td>
<td>1 0</td>
</tr>
<tr>
<td>1 0</td>
<td>1 1</td>
<td>1 1</td>
<td>1 0</td>
<td>1 1</td>
<td>1 1</td>
</tr>
</tbody>
</table>

**Problem 36** A boolean function with two inputs, such as those above, has four input/output pairs. How many different boolean functions of two variables (inputs) exist? How many for a boolean function of three variables?

**Problem 37** Is the representation of a boolean function unique? This means for each of the functions counted above is there only one expression that produces that result?

**Problem 38** Find a function with the same input/output pattern as if \( x \) then \( y \).

**Problem 39** Prove that \( \overline{\overline{x}} = x \).

**Problem 40** Figure out the value for \( f(x) = \frac{n}{x+x+x+\ldots} \) for all integers \( n \).

**Problem 41** Prove that \( x(yz) = (xy)z \).

**Problem 42** Is it possible to solve the following equations for \( x \)?

1. \( x + 1 = 1 \).
2. \( x + y = 1 \).
3.2.1 Duality

Every boolean expression has an alternate called the dual.

**Definition 12 (Boolean Dual)** An expression is the dual of a boolean expression if and only if the expression can be produced by swapping + and · and swapping 0 and 1.

The dual of \( x(y + 1) \) is \( x + (y \cdot 0) \). Note if two boolean expressions are equal, then so also are their duals.

**Problem 43** Choose two, equal, boolean expressions. Find their duals. Show that the duals are equal. You may use functions from above.

3.2.2 Representation

In complicated statements such as those that arise in complicated programming, it is possible to optimize some statements by finding equivalent sets of operations. Boolean function equivalence can be used for this purpose.

First we will consider how to represent arbitrary boolean combinations as boolean functions. First, consider the expression in \( x, y, \) and \( z \) with the value 1 when \( x = y = 1 \) and \( z = 0 \). Because boolean multiplication is only 1 when all factors are one, this expression can be written as \( xy \overline{z} \). Likewise an expression that is 1 when \( x = y = z = 0 \) is \( xy \overline{z} \).

**Problem 44** Find an expression that is 1 when \( x = z = 1 \) and \( y = 0 \). Use the technique above.

Next consider a function \( f(x, y, z) \) defined by the following input/output table.

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>x</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>y</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>z</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>f(x,y,z)</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

Note that this function is 1 exactly when the two expressions above are one. Because \( x + y \) is 1 when either is one, \( f(x, y, z) = xy \overline{z} + x \overline{y} \overline{z} \) is one way to represent this function.

**Problem 45** Find a representation of the following, boolean function.

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>0</th>
<th>1</th>
<th>1</th>
<th>1</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>x</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>y</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>z</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>f(x,y,z)</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

**Problem 46** Remember that boolean functions can be represented as logic statements (and/or/negate) which can be represented as electrical circuits. Design the electrical circuit needed for a light with two switches using the following steps. Note the following supposes that the light is off when both switches are turned down (typical off).

1. Using 0 for down and 1 for up, determine which combinations of up and down results in the light being off (0) and on (1).
2. Write a boolean function for this using the technique above.
3. Convert this boolean function into a logic statement (using ¬, ∨, and ∧).
4. Convert this boolean function into a circuit diagram.

While the mechanism presented above can be used to produce a boolean function or equivalent circuit for any desired combination of inputs and outputs, it does not necessarily produce the most efficient solution. The following example demonstrates how a boolean function can be simplified using the table of identities in Figure 3.1.
The following example demonstrates one way to simplify this boolean function.

\[
\begin{align*}
f(x, y) &= x\overline{y} + xy + y\overline{x} \\
&= x\overline{y} + xy + y\overline{x} \\
&= x\overline{y} + y \cdot (x + \overline{x}) \\
&= x\overline{y} + y \cdot 1 \\
&= x\overline{y} + y \\
&= y + x\overline{y} \\
&= (y + x)(y + \overline{y}) \\
&= (y + x) \cdot 1 \\
&= y + x.
\end{align*}
\]

**Problem 47** Reduce the boolean function \( f(x, y, z) = xy\overline{z} + x\overline{y}z + \overline{x}y\overline{z}. \)
Chapter 4

More Basics

4.1 Modulo Arithmetic

Many concepts in algebra, including cryptography, require arithmetic on finite sets. For the integers there is a relation called modulo arithmetic that defines one such arithmetic.

Definition 13 (Divides) For two integers \(a, b\) \(a\) divides \(b\), denotes \(a|b\) if and only if \(ak = b\) for some integer \(k\).

For example \(2|18\) because \(2 \cdot 9 = 18\).

Definition 14 (Modulo) For three integers \(a, b, n\), \(a\) is equivalent to \(b\) modulo \(n\), denoted \(a \equiv b \mod n\), if and only if \(n|(b − a)\).

For example \(4 \equiv 19 \mod 5\) because \(5|(19 − 4)\) that is \(5 \cdot 3 = 15\).

Problem 48 Determine which of the following are equivalent to \(5 \mod 7\). \(0, 1, 8, 12, 14, 19\)

Problem 49 Find seven (7) numbers equivalent to \(4 \mod 9\).

Problem 50 Using set notation write all numbers equivalent to \(3 \mod 4\).

Problem 51 Select five (5) of the numbers equivalent to \(3 \mod 4\) and divide them by 4. Record the remainder.

Problem 52 Evaluate \(f(n) = n^2 + 2 \mod 4\) at the five numbers equivalent to \(3 \mod 4\) from above. Compare the results.

Lemma 1 Every integer is equivalent to itself \(\mod n\).

Proof: Consider the integer \(k\). Note \(k − k = 0\) and \(n \cdot 0 = 0\). Thus \(k \equiv k \mod n\). \(\square\)

Problem 53 Prove that if \(a \equiv b \mod n\) then \(b \equiv a \mod n\).

Problem 54 Prove that if \(a \equiv b \mod n\) and \(b \equiv c \mod n\) then \(a \equiv c \mod n\).

4.2 Combinatorics: Second Counts

Permutations, presented in Section 1.3.1, count the number of ways to permute, or rearrange, objects. Note that when permuting objects, some can be ignored. For example below are all permutations of two characters from ‘abc’.

ab
ac
ba
bc
c
ca
cb
Problem 55  How many permutations of three letters from the English alphabet (26 characters) are there?

Problem 56  If 10 people participate in a race and only the first three places are recorded, how many possible results are there?

Problem 57  How many permutations of the letters of the word ‘greet’ are there?

4.2.1  Combinations

Sometimes the order of objects is unimportant. The number of outcomes can still be counted.

Problem 58  Suppose 10 people apply for three, identical jobs. How many permutations (ordered) of three selected out of ten are there?

Problem 59  How many ways are there to permute three of three people?

Problem 60  If the first problem counted the number of ways to order three (3) of ten (10) people and the second problem counted the number of ways any particular three can be ordered, how can these be combined to count the number of ways to select three (3) out of ten (10) people?

Problem 61  How many ways are there to select two types of ice cream from a selection of 14?

Problem 62  If a set has 15 elements, how many subsets of 4 elements exist?
Chapter 5

Equivalence Relations

5.1 Relations

With modulo arithmetic any number that is equivalent to another can be substituted in arithmetic without changing the result. This section develops the properties that define equivalence in a general sense.

Definition 15 A subset of a Cartesian product \( R = S \times T \) defines a relation from \( S \) to \( T \).

If \((s, t) \in R\) then \( s \) is related to \( t \) or \( sRt \). Other notations are used to denote elements which are related for specific types of relations as will be seen later. Note a relation can be from a set to itself (e.g., \( R = S \times S \)).

For example consider the relation \( R \) on \( \mathbb{Z} \times \mathbb{Z} \) defined by \((a, b)R(c, d)\) if and only if \( ad = bc \). Thus \((1, 2)(3, 6)\) because \( 1 \cdot 6 = 2 \cdot 3 \).

Definition 16 (Reflexive) A relation \( R \) on a set \( X \) is reflexive if and only if \((a, a) \in R\).

Consider the relation \( R \) on \( \mathbb{Z}^+ \times \mathbb{Z}^+ \) defined by \((a, b)R(c, d)\) if and only if \( ad = bc \). For this relation to be reflexive \((a, b)\) must be related to \((a, b)\). For this relation that requires that \( ab = ba \). This is true by commutativity of real arithmetic. Thus this relation is reflexive.

Next consider the set \( \mathcal{P}(X) \) for some non-empty set \( X \). Let the relation \( R \) be defined by \( A \) is related to \( B \) if and only if \( A \subseteq B \). To show that this is reflexive \((A, A)\) must be in \( R \) for all sets. In this case that means \( A \subseteq A \) for all \( A \in \mathcal{P}(X) \). Note by a previous theorem \( A \subseteq A \) for all sets, thus \( R \) is indeed reflexive.

Problem 63 Let the relation \( R \) on the set of integers be defined by \( aRb \) if and only if \( a \equiv b \mod n \). Note the value of \( n \) is irrelevant here. Prove that this relation is reflexive.

Problem 64 Let the relation \( R \) on the set of integers be defined by \( aRb \) if and only if \( a | b \). Prove that this relation is reflexive.

Problem 65 Let the relation \( R \) on the set of real numbers be defined by \( aRb \) if and only if \( a < b \). Prove that this relation is not reflexive.

Definition 17 (Symmetric) A relation \( R \) on a set \( X \) is symmetric if and only if \((a, b) \in X \) implies \((b, a) \in R\).

Consider the relation \( R \) on \( \mathbb{Z}^+ \times \mathbb{Z}^+ \) defined by \((a, b)R(c, d)\) if and only if \( ad = bc \). For this relation to be symmetric if \((a, b)R(c, d)\) then \((c, d)R(a, b)\). For this relation, \((a, b)R(c, d)\) implies \( ad = bc \). By commutativity of real multiplication \( cb = da \) which means \((c, d)R(a, b)\). Thus this relation is symmetric.

Consider the set \( \mathcal{P}(X) \) for the set \( X = \{a, b, c\} \). Let the relation \( R \) be defined by \( A \) is related to \( B \) if and only if \( A \subseteq B \). To be symmetric if \( A \subseteq B \) then \( B \subseteq A \). However, note that \( \emptyset \subseteq \{a, b, c\} \) so these are related. However \( \{a, b, c\} \not\subseteq \emptyset \) so this relation is not symmetric.

Problem 66 Let the relation \( R \) on the set of integers be defined by \( aRb \) if and only if \( a \equiv b \mod n \). Note the value of \( n \) is irrelevant here. Prove or disprove that this relation is symmetric.
Problem 67  Let the relation $R$ on the set of integers be defined by $aRb$ if and only if $a|b$. Prove or disprove that this relation is symmetric.

Problem 68  Let the relation $R$ on the set of real numbers be defined by $aRb$ if and only if $a \leq b$. Prove or disprove that this relation is symmetric.

Definition 18 (Anti-Symmetric) A relation $R$ on a set $X$ is anti-symmetric if and only if $(a,b), (b,a) \in R$ implies $a = b$.

Consider the relation $R$ on $\mathbb{Z}^+ \times \mathbb{Z}^+$ defined by $(a,b)R(c,d)$ if and only if $ad = bc$. If this is anti-symmetric then there will be no non-trivial symmetric pairs. Consider that $(1,3)R(2,6)$ and $(2,6)R(1,3)$ because $1\cdot 6 = 2\cdot 3$. However $(1,3) \neq (2,6)$. Thus this relation is not anti-symmetric.

Consider the set $\mathcal{P}(X)$ for the set $X = \{a, b, c\}$. Let the relation $R$ be defined by $A$ is related to $B$ if and only if $A \subseteq B$. Note that if $A \subseteq B$ and $B \subseteq A$ then by definition of set equality $A = B$. Thus this relation is anti-symmetric.

Problem 69  Let the relation $R$ on the set of integers be defined by $aRb$ if and only if $a \equiv b \mod n$. Note the value of $n$ is irrelevant here. Prove or disprove that this relation is anti-symmetric.

Problem 70  Let the relation $R$ on the set of integers be defined by $aRb$ if and only if $a|b$. Prove or disprove that this relation is anti-symmetric.

Problem 71  Let the relation $R$ on the set of real numbers be defined by $aRb$ if and only if $a \leq b$. Prove or disprove that this relation is anti-symmetric.

Definition 19 (Transitive) A relation $R$ on a set $X$ is transitive if and only if $(a,b) \in R$ and $(b,c) \in R$ implies $(a,c) \in R$.

Consider the relation $R$ on $\mathbb{Z}^+ \times \mathbb{Z}^+$ defined by $(a,b)R(c,d)$ if and only if $ad = bc$. For this relation to be transitive $(a,b)R(c,d)$ and $(c,d)R(e,f)$ then $(a,b)R(e,f)$. Note $(a,b)R(c,d)$ means $ad = bc$. Also $(c,d)R(e,f)$ means $cf = de$.

\[
\begin{align*}
ad &= bc. \\
ad/b &= c. \\
c/f &= de. \\
ad/b \cdot c/f &= de. \\
ad/c &= deb. \\
ad/b \cdot c/f &= eb. \\
a/f &= eb. \\
= &= be.
\end{align*}
\]

This last implies that $(a,b)R(e,f)$. Thus this relation is transitive.

Consider the set $\mathcal{P}(X)$ for the set $X = \{a, b, c\}$. Let the relation $R$ be defined by $A$ is related to $B$ if and only if $A \subseteq B$. To show that this is transitive requires showing that if $(A, B), (B, C) \in R$ then $(A, C) \in R$. For this relation this means that if $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$. This has been proven in a previous problem, thus the relation is transitive.

Problem 72  Let the relation $R$ on the set of integers be defined by $aRb$ if and only if $a \equiv b \mod n$. Note the value of $n$ is irrelevant here. Prove or disprove that this relation is transitive.

Problem 73  Let the relation $R$ on the set of integers be defined by $aRb$ if and only if $a|b$. Prove or disprove that this relation is transitive.

Problem 74  Let the relation $R$ on the set of real numbers be defined by $aRb$ if and only if $a \leq b$. Prove or disprove that this relation is transitive.
5.2 Equivalence Relations

Definition 20 (Equivalence Relation) A relation is an equivalence relation if and only if the relation is reflexive, symmetric, and transitive.

Problem 75 Prove or disprove that the following relation is an equivalence relation. Consider the set \( P(X) \) for the set \( X = \{a, b, c\} \). Let the relation \( R \) be defined by \( A \) is related to \( B \) if and only if \( A \subseteq B \).

Problem 76 Prove or disprove that the following relation is an equivalence relation. Let the relation \( R \) on the set of integers be defined by \( aRb \) if and only if \( a \equiv b \mod n \). Note the value of \( n \) is irrelevant here.

Problem 77 Prove or disprove that the following relation is an equivalence relation. Let the relation \( R \) on the set of integers be defined by \( aRb \) if and only if \( a \mid b \).

Problem 78 Prove or disprove that the following relation is an equivalence relation. Let the relation \( R \) on the set of real numbers be defined by \( aRb \) if and only if \( a \leq b \).

5.3 Equivalence Classes

Definition 21 (Equivalence Class) For an equivalence relation \( R \), a set of elements, denoted \([y]\), is an equivalence class if and only if \( \{x \mid xRY\} \).

Consider the relation \( R \) on \( \mathbb{Z}^+ \times \mathbb{Z}^+ \) defined by \((a, b)R(c, d) \) if and only if \( ad = bc \). The equivalence class of \([1, 2]\) = \{(1, 2), (2, 4), (3, 6), \ldots\}. The equivalence class of \([5, 3]\) = \{(5, 3), (10, 6), (15, 9), \ldots\}.

Problem 79 Find the equivalence classes of 0 and 1 for the relation \( a \equiv b \mod 5 \).

Consider the following equivalence relation. \( X = \{mx + b \mid m, b \in \mathbb{R}\} \), the set of all 2D lines. \( R \) is defined by \( \ell_1(x) = m_1x + b_1 \equiv \ell_2(x) = m_2x + b_2 \) if and only if \( m_1 = m_2 \).

Problem 80 Find the equivalence classes of \( y = 5x + 3 \) and \( y = \frac{11}{7}x + \frac{13}{208} \).
Chapter 6

Partially Ordered Sets

6.1 Definition

Definition 22 (Poset) A relation is an partially ordered set (poset) if and only if the relation is reflexive, antisymmetric, and transitive.

Problem 81 Prove or disprove that the following relation is a poset. Consider the set $\mathcal{P}(X)$ for the set $X = \{a, b, c\}$. Let the relation $R$ be defined by $A$ is related to $B$ if and only if $A \subseteq B$.

Problem 82 Prove or disprove that the following relation is a poset. Let the relation $R$ on the set of integers be defined by $aRb$ if and only if $a \equiv v \mod n$. Note the value of $n$ is irrelevant here.

Problem 83 Prove or disprove that the following relation is a poset. Let the relation $R$ on the set of integers be defined by $aRb$ if and only if $a|b$.

Problem 84 Prove or disprove that the following relation is a poset. Let the relation $R$ on the set of real numbers be defined by $aRb$ if and only if $a \leq b$.

6.2 Representation

Consider the following poset. $R = \{(a, a), (b, b), (c, c), (d, d), (a, b), (a, c), (a, d), (b, d), (c, d)\}$. The following is called the Hasse diagram for $R$. Note that it does not depict the reflexive relations (assumed) nor the transitive ones (directly).

![Hasse Diagram](image.png)

Figure 6.1: Hasse Diagram

Problem 85 Draw the Hasse diagrams for the following posets.
1. \( \subseteq \) on \( P(\{0,1\}) \). Note it may help to list all the elements first.

2. | (i.e., \( aRb \) iff \( a|b \)) on \( \{1,2,3,6\} \).

3. | on \( \{1,2,3,5,6,10,15,30\} \).

4. \( X = \{(0,0,0),(1,0,0),(0,1,0),(0,0,1),(0,1,1),(1,0,1),(1,1,0),(1,1,1)\} \) with the relation 
   \((a_1,a_2,a_3) \leq (b_1,b_2,b_3) \) iff \( a_i \leq b_i \) for all \( i \).

6.3 Properties

**Definition 23 (Comparable)** Two elements \( a,b \) of a poset are comparable if and only if either \( a \leq b \) or \( b \leq a \).

**Problem 86** Find two comparable elements in each of the relations in Problem 85.

**Problem 87** Find two incomparable elements in each of the relations in Problem 85.

**Definition 24 (Total Ordering)** A partially ordered set is a totally ordered set if and only if all pairs of elements are comparable.

**Definition 25 (Least Upper Bound)** An element \( c \) is a least upper bound of two elements \( a \) and \( b \), denoted \( a \wedge b \), if and only if \( a \leq c \), \( b \leq c \) and if \( a \leq d \), \( b \leq d \) for any other element then \( c \leq d \).

**Definition 26 (Greatest Lower Bound)** An element \( c \) is a greatest lower bound of two elements \( a \) and \( b \), denoted \( a \vee b \), if and only if \( c \leq a \), \( c \leq b \) and if \( d \leq a \), \( d \leq b \) for any other element then \( d \leq c \).

**Problem 88** Consider the poset \( | \) on \( \{1,2,3,5,6,10,15,30\} \).

1. Find \( 2 \wedge 5 \)
2. Find \( 10 \vee 15 \)
3. Find \( 2 \wedge 6 \)

**Definition 27 (Maximal Element)** An element \( a \) in a poset is a maximal element if and only if there does not exist an element \( b \) such that \( a \leq b \).

**Definition 28 (Minimal Element)** An element \( a \) in a poset is a minimal element if and only if there does not exist an element \( b \) such that \( b \leq a \).

**Problem 89** Find all minimal and maximal elements of the posets in Problem 85.

6.4 Lattice

**Definition 29 (Lattice)** A partially ordered set is a lattice if and only if every pair of elements has a least upper bound and a greatest lower bound.

**Problem 90** Determine if each of the posets in Problem 85 is a lattice.
Chapter 7

More Proofs

7.1 Contradiction

Sometimes starting with the condition and working directly to the conclusion is too difficult when devising a proof. Given that a statement is either true or false, another approach is to start with the condition and suppose the conclusion to be false. If this leads to an error—a contradiction of a known statement—then the supposition of falsehood is false. Yes, this is proof by double negative. Consider the following example.

There exists a unique positive integer \(e\) such that \(e|n\) for all positive integers \(n\).

Proof: Suppose, for sake of contradiction, that there is more than one integer that divides all positive integers. If there is more than one, than there exists positive integers \(e\) and \(f\) such that \(e|n\) and \(f|n\) for all positive integers \(n\).

Thus \(e|f\) and \(f|e\). By definition of divides

\[
\begin{align*}
e k &= f, \\
f j &= e, \\
(ek)j &= e, \text{ by substitution.} \\
e(kj) &= e, \text{ commutativity of arithmetic.} \\
k j &= 1, \text{ integer identity.} \\
k &= 1. \\
e &= f, \text{ by substitution.}
\end{align*}
\]

Thus the supposition that there exists more than one is false. There is a unique positive integer \(e\) such that \(e|n\) for all positive integers \(n\). \(\square\)

Problem 91  Prove that for any poset the least upper bound of two elements is unique.

Definition 30 (Maximum Element) An element \(m\) in a poset is a maximum element if and only if \(\forall a, a \preceq m\).

Problem 92  Prove that for any poset a maximum element, if it exists, is unique.

Problem 93  Prove that for any poset if a maximum element exists, there is only one maximal element.

7.2 Functions

Definition 31 (Function) A mapping (relation) is a function if and only if for each input there exists exactly one output.

The following are examples of functions.

- From \(\mathbb{Z}_5 \rightarrow \mathbb{Z}_5\) \(f_1 = \{(0, 0), (1, 1), (2, 4), (3, 4), (4, 1)\}\)
• From $\mathbb{Z}_5 \rightarrow \mathbb{Z}_5$ $f_2 = \{(0, 4), (1, 3), (2, 2), (3, 1), (4, 0)\}$

• From $\mathbb{Z}_5 \rightarrow \mathbb{Z}_5$ $f_3 = 3n + 1.$

The mapping from $\mathbb{Z}_5 \times \mathbb{Z}_5$ $g = \{(0, 0), (0, 2), (1, 1), (1, 3), (2, 2), (2, 4), (3, 3), (3, 0), (4, 4), (4, 1)\}$ is not a function. Remember that a relation is a subset of a Cartesian product $D \times C.$ For a function the first set $D$ is called the domain and the second set $C$ is called the codomain. For a function $f$ that is a subset of $D \times C$ the set $R = \{(c|(d, c) \in f\}$ is called the range.

**Problem 94** Determine which of the following are functions.

1. $r_1: \mathbb{Z}_5 \rightarrow \mathbb{Z}_5$ given by $r_1 = \{(0, 2), (1, 3), (2, 0), (3, 4), (4, 1)\}$

2. $r_1: \mathbb{Z}_5 \rightarrow \mathbb{Z}_5$ given by $r_2 = \{(0, 1), (1, 2), (2, 3), (3, 4), (4, 0), (0, 4)\}$

3. $r_3: \mathbb{R} \rightarrow \mathbb{R}$ given by $r_3 = \{(d, c) : c = d^4\}$

4. $r_4: \mathbb{R} \rightarrow \mathbb{R}$ given by $r_4 = \{(d, c) : c^2 = d\}$

**Definition 32 (Onto)** A function $f: D \rightarrow C$ is onto if and only if the range of $f$ is $C$

$f : \mathbb{R} \rightarrow \mathbb{R}$ given by $f(x) = 5x - 3$ is onto, because for any $y \in \mathbb{R}$

\[
\begin{align*}
y & = 5x - 3. \\
y + 3 & = 5x. \\
\frac{1}{5}(y + 3) & = x.
\end{align*}
\]

Thus there is a domain element for each codomain element.

$g : \mathbb{R} \rightarrow \mathbb{R}$ given by $g(x) = x^2$ is not onto, because $-1 \in \mathbb{R}$ but is not in the range of $g.$

**Definition 33 (One-to-one)** A function $f: D \rightarrow C$ is one-to-one if and only if $f(a) = f(b)$ implies $a = b.$

$f : \mathbb{R} \rightarrow \mathbb{R}$ given by $f(x) = 5x - 3$ is one-to-one, because

\[
\begin{align*}
f(a) & = f(b), \text{ implies} \\
5a - 3 & = 5b - 3. \text{ Hence,} \\
5a & = 5b, \text{ and} \\
a & = b.
\end{align*}
\]

$g : \mathbb{R} \rightarrow \mathbb{R}$ given by $g(x) = x^2$ is not one-to-one because $g(2) = g(-2)$ and $2 \neq -2.$

**Definition 34 (Bijection)** A function is a bijection if and only if it is one-to-one and onto.

**Problem 95** Determine if each of the following is one-to-one and if they are onto.

1. $r_1: \mathbb{Z}_5 \rightarrow \mathbb{Z}_5$ given by $r_1 = \{(0, 2), (1, 3), (2, 0), (3, 4), (4, 1)\}$

2. $r_3: \mathbb{R} \rightarrow \mathbb{R}$ given by $r_3(d) = d^4$

3. $r_4: \mathbb{Z} \rightarrow \mathbb{Z}$ given by $r_4(n) = 2n$

4. Person from table People—people who work or attend classes at UAA—to their UAA ID (8 digit unique key).

5. class from the table People (everyone with a UAA ID) to table Enrollment (every ID, class, semester combination).

**Definition 35 (Inverse Mapping)** A mapping $g : C \rightarrow D$ is the inverse mapping of a mapping $f$ if and only if $g = \{(c, d) : (d, c) \in f\}.$
For the function
\[ r_1 = \{(0, 2), (1, 3), (2, 0), (3, 4), (4, 1)\} \]
the inverse mapping is
\[ r_1^{-1} = \{(2, 0), (3, 1), (0, 2), (4, 3), (1, 4)\} \].

Note that \( r_1^{-1} \) is also a function. Thus this is an inverse function, not just an inverse mapping. For the function \( r_3(d) = d^4 \), however, the inverse mapping contains the elements \((1, 1)\) and \((1, -1)\). Thus this inverse mapping is not a function.

**Theorem 1** If a function is one-to-one, then the inverse mapping is a function.

Proof: Let \( f \) be a one-to-one function. Let \( f^{-1} \) be the inverse mapping for \( f \). Suppose for the sake of contradiction that \( f^{-1} \) is not a function. By definition of function this means that there exist elements \((a, b), (a, c) \in f^{-1}\) where \( b \neq c \). This implies that \( f(b) = f(c) \) by definition of inverse mapping. However \( b \neq c \) contradicts the definition of one-to-one. Thus if a function is one-to-one, its inverse mapping is a function.

**Problem 96** Prove that if a function has an inverse function, that inverse function is unique.

Functions can be applied in sequence. If \( f_1 : A_1 \to A_2 \) and \( f_2 : A_2 \to A_3 \), then after \( f_1 \) maps an \( a \in A_1 \) to an \( b \in A_2 \), then \( f_2 \) can map that \( b \) to \( c \in A_3 \). This is denoted \((f_2 \circ f_1)(a) = c \) or \( f_2(f_1(a)) = c \).

**Problem 97** Prove that if \( f \) has an inverse function \( f^{-1} \) then \( f \circ f^{-1} \) and \( f^{-1} \circ f \) are the identity function.
Chapter 8

Graph Theory

8.1 Definition

There are different types of graphs each of which represents different types of data. For this chapter all graphs will be simple graphs whose properties can be discovered below.

Definition 36 Two vertices, $v_i$ and $v_j$, in a graph $G$ are adjacent if and only if $v_i v_j$ is an edge in $G$.

Definition 37 Two edges in a graph $G$ are incident if and only if they share a vertex.

Problem 98 Complete the Figures above labeled “Which of these are graphs?” (Figures 8.3 and 8.6)

Problem 99 In terms of the diagrams list properties required and properties not allowed in graphs.

Problem 100 In terms of the sets list properties required and properties not allowed in graphs.

Problem 101 Draw the diagram form of the first graph in Figure 8.4
8.2 Graph Properties

Definition 38 (Degree) The degree of a vertex \( v \) is the number of edges incident with \( v \).

Problem 102 Prove that the sum of the degrees of all vertices equals twice the number of edges.

Problem 103 Prove that the number of vertices of odd degree is even.

The minimum degree of all vertices in a graph \( G \) is denoted \( \delta(G) \) and the maximum degree of all vertices in a graph \( G \) is denoted \( \Delta(G) \).

Problem 104 List the minimum and maximum degree of every graph in Figure 8.9.
Problem 105 Determine which graphs in Figure 8.7 are regular.

**Definition 39 (Regular)** A graph $G$ is regular if and only if the degree of all vertices are the same.

Figure 8.7 shows a regular graph.

**Problem 105** Determine which graphs in Figure 8.7 are regular.
Definition 40 (Subgraph) A graph $H = (V_H, E_H)$ is a subgraph of a graph $G = (V_G, E_G)$ if and only if $V_H \subseteq V_G$ and $E_H \subseteq E_G$.

Definition 41 (Complete Graph) A graph $G$ with $|V| = n$ is a complete graph, denoted $K_n$, if and only if $(v_i, v_j) \in E$ for all $i \neq j$.

Complete graphs are also known as cliques. The complete graph on five vertices, $K_5$, is shown in Figure 8.8. The size of the largest clique in a graph is called the clique number, denoted $\Omega(G)$.

Problem 106 Find $\Omega(G)$ for every graph in Figure 8.7.

Problem 107 Prove that a complete graph is regular.

Definition 42 (Independent Set) A set of vertices in a graph are independent if and only if there are no pair of the vertices are adjacent.

The size of the maximum independent set in a graph $G$ is denoted $\alpha(G)$.

Problem 108 Find $\alpha(G)$ for every graph in Figure 8.7.

Problem 109 Re-write the definition of independent set exchanging vertices for edges. Note this is called a matching.

Problem 110 Find the size of the maximum matching for each graph in Figure 8.9.

Definition 43 (Bipartite Graph) A graph $G$ is bipartite if and only if the vertices can be partitioned into two sets such that no two vertices in the same partition are adjacent.

Problem 111 Determine which graphs in Figure 8.9 are bipartite.
8.3. ISOMORPHISM

Note that if each vertex in any partition of a bipartite graph is adjacent to all vertices in the other partition the graph is called complete bipartite and is denoted $K_{n,m}$ where $n,m$ are the sizes of the partitions.

Problem 112 Write a definition for tripartite graphs.

Definition 44 (Graph Complement) The complement of a graph $G = (V, E)$ is the graph $H = (V, E_2)$ such that $v_1, v_2$ are adjacent in $H$ if and only if they are not adjacent in $G$.

Problem 113 Construct the graph complement of the first graph in Figure 8.10.

Problem 114 Construct the graph complement of $K_4$.

Definition 45 (Graph Dual) The dual of a graph $G = (V, E)$ is the graph $H = (E, E_2)$ such that for two vertices (edges of $G$) are adjacent if they were incident in $G$.

Problem 115 Construct the graph complement of the first graph in Figure 8.10.

8.3 Isomorphism

When calculating properties of the graphs in Figures 8.9 and 8.10 you may have noted that some of the graphs shared many properties. It should also be apparent that a given graph can be drawn in many different ways given that the relative location of vertices and shape of edges is irrelevant. If two graphs are essentially the same, they are called isomorphic.

Definition 46 (Graph Isomorphism) Two graphs $G = (V_G, E_G)$ and $H = (V_H, E_H)$ are isomorphic if and only if there exists a bijection $f : V_G \to V_H$ such that if $\{v_1, v_2\} \in E_G$ then $\{f(v_1), f(v_2)\} \in E_H$.

Problem 116 Determine and prove which graphs in Figures 8.9 and 8.10 are isomorphic.

8.4 Paths

Definition 47 (Walk) A graph is a walk if and only if the vertices can be labeled $v_0, v_1, \ldots, v_k$ such that $v_i, v_{i+1}$ is an edge.

Definition 48 (Trail) A graph is a trail if and only if it is walk such that no edge is used twice.

Definition 49 (Path) A graph is a path if and only if it is walk such that no vertex is used twice.

Please note that these terms vary widely including switching the names, so always check the definition in the article, book, or other material you are reading.

Problem 117 Draw a path of length 5. Note this is denoted $P_5$.

Problem 118 Draw a walk that is not a trail.

Problem 119 Draw a trail that is not a path.

Definition 50 (Eulerian Trail) A trail is Eulerian if and only if it uses every edge in the graph.

Definition 51 (Hamiltonian Path) A path is Hamiltonian if and only if it uses every vertex in that graph.

Problem 120 Determine which graphs in Figure 8.7 have Eulerian trails.

Problem 121 Determine which graphs in Figure 8.7 have Hamiltonian paths.
8.5 Connected

**Definition 52 (Connected)** A graph $G$ is connected if and only if for every pair of vertices $v, w$ there exists a path from $v$ to $w$.

**Problem 122** Determine which of the graphs in Figure 8.1 are connected.

**Problem 123** Prove that every complete graph is connected.

**Problem 124** Prove that every complete bipartite graph is connected.

**Problem 125** Determine if every bipartite graph must be connected.
Definition 53 (\(n\)-connected) A graph \(G\) is \(n\)-connected if and only if \(n\) is the minimum number of vertices that can be removed resulting in a disconnected graph.

Problem 126 For each of the graphs in Figure 8.9 and 8.10 determine the maximum \(n\) for which the graph is \(n\)-connected.

Problem 127 If a graph is \(n\)-connected what does this say about the minimum of the number of paths between any two vertices?

8.6 Cycles

Definition 54 (Circuit) A graph is a circuit, or closed walk, if and only if the vertices can be labeled \(v_0, v_1, \ldots, v_k\) such that \(\{v_j, v_{j+1}\}\) is an edge for all \(j\) and \(v_0 = v_k\).

Definition 55 (Simple Circuit) A graph is a simple circuit, or simple closed walk, if and only if it is a circuit such that no edge is used twice.

Definition 56 (Cycle) A graph is a cycle if and only if it is a circuit such that no vertex is used twice.

Please note that as with paths the terms vary widely.

Problem 128 Draw a cycle of length 4. Note this is denoted \(C_4\).

Problem 129 Draw a circuit that is not a simple circuit.

Problem 130 Draw a simple circuit that is not a cycle.
Definition 57 (Eulerian Circuit) A simple circuit is Eulerian if and only if it uses every edge in the graph.

Definition 58 (Hamiltonian Circuit) A simple circuit is Hamiltonian if and only if it uses every vertex in that graph.

Problem 131 Determine which graphs in Figure 8.9 have Eulerian circuits.

Problem 132 Determine which graphs in Figure 8.9 have Hamiltonian circuits.

8.7 Trees

Definition 59 (Tree) A graph is a tree if and only if it is connected and contains no cycles.

Problem 133 Determine which graphs in Figure 8.7 are trees.

Problem 134 Draw all non-isomorphic trees on 3 vertices.

Definition 60 (Leaf) A vertex in a tree is a leaf if and only if it has degree one.

Problem 135 Prove that every tree with at least two vertices has at least one leaf.

Problem 136 Draw a tree with 7 vertices. Determine the maximum $n$ for which the tree is $n$-connected.

Problem 137 Prove that for any tree removal of a leaf produces another tree.

Definition 61 (Spanning Tree) A graph $G$ is a spanning tree of a graph $H$ if and only if $G$ is a subgraph of $H$ that contains all the vertices of $H$ and is a tree.

Problem 138 Find a spanning tree for every graph in Figure 8.7.
Chapter 9

More Enumeration

9.1 Inclusion/Exclusion

Sometimes to count possibilities it is easier to over count and then count how much the over count was and fix it. For example, consider the size of the union of two sets $A$ and $B$ as shown in Figure 9.1. Note that $|A| + |B|$ over counts the size of the union by precisely $|A \cap B|$. Thus the correct count is $(|A| + |B|) - |A \cap B|$.

This can be extended to three sets. See Figure 9.2. This time there are three pairs of sets that overlap. Thus the count starts $(|A| + |B| + |C|) - (|A \cap B| + |A \cap C| + |B \cap C|)$. However this removes $|A \cap B \cap C|$ three times. Thus the correct count is $(|A| + |B| + |C|) - (|A \cap B| + |A \cap C| + |B \cap C|) + |A \cap B \cap C|$.

Problem 139 Write the formula for the number of elements in the union of four, distinct sets.

Because this process first includes (adds) everything, next excludes (subtracts) some things, then includes (adds) other things, the technique is called inclusion/exclusion.

Definition 62 (Derangement) A permutation is a derangement if no element is in its original position.

For example ‘het’ is a derangement of ‘the’, but ‘teh’ is not a derangement.

Problem 140 Count all derangements of ‘one’.

Problem 141 Count all derangements of ‘four’.

Problem 142 Count the number of multiples of 2,3,5 that are less than 100.
**Problem 143** If you know the number of distinct students who took MATH A231 in the Fall 2014 semester, the number of distinct students who took CSCE A241 in the Fall 2014 semester, what do you need to know the total number of distinct students who took either MATH A231 or CSCE A241 in the Fall 2014 semester?

**Problem 144** If you know the following, what do you still need to know to determine the number of distinct students placing into MATH A054, PRPE A080, or having an SAT score below 1290?

1. Number of distinct students taking MATH A054.
2. Number of distinct students taking PRPE A080.
3. Number of distinct students with SAT score below 1290.

### 9.2 Recursion Relations

Sometimes directly counting can be difficult. Consider the following famous example from Fibonacci’s *Liber Abaci*.

The first month there was one pair of rabbits. The second month there was still one pair of rabbits. Starting the third month and continuing every month thereafter, the number of pairs of rabbits is the sum of the previous two months. Thus the third month there are 1 + 1 = 2 pairs of rabbits. The fourth month there are 1 + 2 = 3 pairs of rabbits. This produces the following sequence.

\[1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots\]

Because each element of this sequence is expressed in terms of previous elements, the sequence is *recursive*. The Fibonacci sequence in standard notation is

\[a_1 = 1, \ a_2 = 1, \ a_n = a_{n-1} + a_{n-2}\]

While it is possible to produce a function that provides the \(n\)th term, this is not easy.

Next consider the number of words from the alphabet \{a,b,c,d,e\} with no two, consecutive a’s. For words of length one there are no restrictions, so there are 5. For words of length two all combinations except ‘aa’ are acceptable. Thus there are 25 - 1 = 24 words of length two. For words of length three all combinations except ‘aaa’, ‘aaX,’ and ‘Xaa’ are allowable. This removes 1 + 4 + 4 = 9 words leaving 5\(^3\) - 9 = 116 acceptable words.

For longer words of length \(n\), note that removing the last letter produces an acceptable word of length \(n-1\). Appending b,c,d,e to the end of these words produces another acceptable word.

If the last letter of the word of length \(n-1\) is a, then the previous letter is not (4 options). This leaves any word of length \(n-3\). Thus there are 4\(a_{n-3}\) words of length \(n-1\) ending in a. For each of these there are four words of length \(n\) (ending in b,c,d,e).
Thus the total number of acceptable words of length $n$ is

$$a_n = 4a_{n-1} + 16a_{n-3}.$$ 

**Problem 145** Guido is superstitious and will not take food from two, adjacent bins at a buffet. If the buffet is a line having $n$ bins each containing distinct food, how many different combinations of food can he choose? Note he can eat as many items as he wants.

**Problem 146** Guido walks up stairs taking one or two steps at a time. Find a recursive formula for the number of ways he could end up at step $n$. Note he starts at step 0 (not on the stairs).

### 9.3 Induction

Recursion relations provide an easier way to express some sequences. Similarly a proof technique known as mathematical induction provides an easier way to prove some theorems including theorems about recurrence relations.

Consider the following example.

The $n$th element of the Fibonacci sequence is

$$f(n) = \frac{1}{\sqrt{5}} \left( \left( \frac{1 + \sqrt{5}}{2} \right)^n - \left( \frac{1 - \sqrt{5}}{2} \right)^n \right).$$

Proof: The following is a proof by mathematical induction on the index $n$.

**Basis step:** The following demonstrates that the formula works for $n = 1, 2$.

- $f(1) = \frac{1}{\sqrt{5}} \left( \left( \frac{1 + \sqrt{5}}{2} \right)^1 - \left( \frac{1 - \sqrt{5}}{2} \right)^1 \right)$
  - $= \frac{1}{\sqrt{5}} \left( \frac{1 + \sqrt{5}}{2} - \frac{1 - \sqrt{5}}{2} \right)$
  - $= \frac{1}{\sqrt{5}} \left( \frac{2\sqrt{5}}{2} \right)$
  - $= 1.$

- $f(2) = \frac{1}{\sqrt{5}} \left( \left( \frac{1 + \sqrt{5}}{2} \right)^2 - \left( \frac{1 - \sqrt{5}}{2} \right)^2 \right)$
  - $= \frac{1}{\sqrt{5}} \left( \frac{3 + \sqrt{5}}{2} - \frac{3 - \sqrt{5}}{2} \right)$
  - $= \frac{1}{\sqrt{5}} \left( \frac{2\sqrt{5}}{2} \right)$
  - $= 1.$

Thus the formula works for $n = 1, 2$.

**Induction step:** The following demonstrates that the formula works for $n$ if it works for $n - 1$ and $n - 2$.

Suppose $a_{n-1} = f(n - 1)$ and $a_{n-2} = f(n - 2)$. By definition of the Fibonacci sequence

$$a_n = a_{n-1} + a_{n-2}$$

$$= f(n - 1) + f(n - 2)$$

$$= \frac{1}{\sqrt{5}} \left( \left( \frac{1 + \sqrt{5}}{2} \right)^{n-1} - \left( \frac{1 - \sqrt{5}}{2} \right)^{n-1} \right) + \frac{1}{\sqrt{5}} \left( \left( \frac{1 + \sqrt{5}}{2} \right)^{n-2} - \left( \frac{1 - \sqrt{5}}{2} \right)^{n-2} \right)$$
Thus the formula works for \( n \) if it works for \( n - 1 \) and \( n - 2 \).

Because the formula works for \( n = 1, 2 \) and because the formula recurses, by the principle of mathematical induction, the statement is true.

\[ \text{Problem 147} \quad \text{Prove that any tree on } n \text{ vertices has } n - 1 \text{ edges.} \]

\[ \text{Problem 148} \quad \text{Prove that } \sum_{i=1}^{n} i = \frac{n(n+1)}{2}. \]

\[ \text{Problem 149} \quad \text{Find and prove a formula for the number of regions a plane is divided into by } n \text{ lines no two of which are parallel. Note regions may be finite or infinite.} \]
Appendix A

Appendix

A.1 UA Database

<table>
<thead>
<tr>
<th>Person</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>8 digit integer, unique key</td>
</tr>
<tr>
<td>First Name</td>
<td>string</td>
</tr>
<tr>
<td>Last Name</td>
<td>string</td>
</tr>
<tr>
<td>Middle Name</td>
<td>string</td>
</tr>
<tr>
<td>Birth Year</td>
<td>integer</td>
</tr>
<tr>
<td>Birth Month</td>
<td>integer</td>
</tr>
<tr>
<td>Birth Day</td>
<td>integer</td>
</tr>
<tr>
<td>Ethnicity</td>
<td>string</td>
</tr>
<tr>
<td>Major 1</td>
<td>string 5</td>
</tr>
<tr>
<td>Major 2</td>
<td>string 5</td>
</tr>
<tr>
<td>Minor 1</td>
<td>string 5</td>
</tr>
<tr>
<td>Minor 2</td>
<td>string 5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Course</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CRN</td>
<td>5 digit integer</td>
</tr>
<tr>
<td>Year</td>
<td>integer</td>
</tr>
<tr>
<td>Campus</td>
<td>string length 1</td>
</tr>
<tr>
<td>Prefix</td>
<td>string length 4</td>
</tr>
<tr>
<td>Course</td>
<td>string length 4</td>
</tr>
<tr>
<td>Section</td>
<td>string length 3</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Transcript</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>8 digit integer</td>
</tr>
<tr>
<td>CRN</td>
<td>5 digit integer</td>
</tr>
<tr>
<td>Year</td>
<td>integer</td>
</tr>
<tr>
<td>Grade</td>
<td>string length 1</td>
</tr>
<tr>
<td>Last Day</td>
<td>date</td>
</tr>
</tbody>
</table>