Lecture Notes: Mathematical/Discrete Structures

Rashid Bin Muhammad, PhD.

This booklet includes lecture notes, homework problems, and exam problems from discrete structures course I taught in Fall 2006 at the Kent State University, USA. I wrote a good part of these notes in Fall 2006; I revise them every time I teach the course. The problems in the notes have been used in class lectures, homework assignments, or exams. You can find a collection of homework assignments and exams from past semesters of my class online at http://www.personal.kent.edu/~rmuhamma/.

Please do not ask for solutions. If you are a student, the only way to learn the material is solve yourself. If you are a teacher, you should not assign problems that you cannot solve yourself.

Propositional Logic

1 Introduction

The algorithms in computer science and proofs in mathematics use logical expressions such as "if p then q". Therefore, it is neccessary to know the truth value of such expressions, that is, to know the cases in which these expressions are either true or false. We discuss these issues in this lecture.

1.1 Proposition

A proposition (or statement) is a sentence that is true or false but not both.

Example. (1) $2+2=4$ (proposition). (2) $5+2=7$ (proposition). (3) $x+2=7$ (not a proposition). (4) He will go to school. (not a proposition).

1.2 Compound Proposition

Many propositions are composite, that is, composed of subpropositions and various connectives. Such composite propositions are called compound propositions.

1.3 Primitive Proposition

If proposition cannot be broken down into simpler propositions, that is, if it is not composite.

1.4 Basic Logical Operations

This section discusses the three basic logical operations of conjunction, disjunction, and negation.

1.4.1 Conjunction

If p and q are proposition variables, the conjunction of p and q is "p and q." It is true when, and only when, both p and q are true. If either p or q is false, or if both are false, $p \wedge q$ is false.

p	q	$p \wedge q$
T	T	T
T	F	F
F	T	F
F	F	F

1.4.2 Disjunction

If p and q are proposition variables, the disjunction of p and q is "p or q." It is true when at least one of p or q is true and false only when both p and q are false.

p	q	$p \vee q$
T	T	T
T	F	T
F	T	T
F	F	F

1.4.3 Negation

If p is a proposition variable, the negation of p is "not p" or "It is not the case that p" and denoted $\sim p$. It has opposite truth value from p: if p is true, $\sim p$ is false; if p is false, $\sim p$ is true.

p	$\sim p$
T	F
F	T

1.5 Proposition Form

A proposition form is an expression made up of proposition variables and logical connectives that becomes a proposition when actual propositions are substituted for the component proposition variable. The truth table for a given proposition form displays the truth values that correspond to the different combinations of truth values for the variables.

Example. (1)$(p \vee q) \wedge \sim (p \wedge q)$. (2)$(p \wedge q) \vee \sim r$.

1.6 Logical Equivalence

Two proposition forms are called logically equivalent if, and only if, they have identical truth values for each possible substitution of propositions for their proposition variables. The logical equivalence of proposition forms P and Q is denoted by writing $P \equiv Q$.

Example. (1) Double Negative Property: $\sim (\sim p)$. (2) Show Nonequivalence: $\sim (p \wedge q)$ and $\sim p \wedge \sim q$.

1.6.1 De Morgan's Laws

The following two logical equivalences are known as De Mogan's laws of logic.

The negation of an and proposition is logically equivalent to the or proposition in which each component is negated. Symbolically, $\sim (p \wedge q) \equiv \sim p \vee \sim q$. On the other hand, the negation of an or proposition is logically equivalent to the and proposition in which each component is negated. Symbolically, $\sim (p \vee q) \equiv \sim p \wedge \sim q$.

Example. Inequalities and De Morgan's Laws.

1.7 Tautologies and Contradictions

A *tautology* is a proposition form that is always true regardless of the truth values of the individual propositions substituted for its proposition variables. A proposition whose form is a tautology is called a tautological proposition.

A *contradiction* is a proposition form that is always false regardless of the truth values of the indivitual stateemnts substituted for its proposition variables. A proposition whose form is a contradiction is called a contradictory proposition.

Example. (1) Show that the proposition form $p \vee \sim p$ is a tautology. (2) Show that the proposition form $p \wedge \sim p$ is a contradiction.

1.8 Logical Equivalences

Theorem 1. *Given any proposition variables p, q, and r, a tautology t and a contradiction c, the following logical equivalences hold:*

1. Commutative Laws

$$p \wedge q \equiv q \wedge p$$

$$p \vee q \equiv q \vee p$$

2. Associative Laws

$$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$$

$$(p \vee q) \vee r \equiv p \vee (q \vee r)$$

3. Distributed Laws

$$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$$

$$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$$

4. Identtity Laws

$$p \wedge t \equiv p$$

$$p \vee c \equiv p$$

5. Negation Laws

$$p \vee \sim p \equiv t$$

$$p \wedge \sim p \equiv c$$

6. Double Negation Law

$$\sim (\sim p) \equiv p$$

7. Idempotent Laws

$$p \wedge p \equiv p$$

$$p \vee p \equiv p$$

8. De Morgan's Laws

$$\sim (p \wedge q) \equiv \sim p \vee \sim q$$

$$\sim (p \vee q) \equiv \sim p \wedge \sim q$$

9. Universal Bound Laws

$$p \vee t \equiv t$$

$$p \wedge c \equiv c$$

10. Absorption Laws

$$p \vee (p \wedge q) \equiv p$$

$$p \wedge (p \vee q) \equiv p$$

11. Negations of t and c

$$\sim t \equiv c$$

$$\sim c \equiv t$$

1.9 Conditional Proposition

If p and q are proposition variables, the *conditional* of q by p is "if p then q" or "p implies q." It is false when p is true and q is false; otherwise it is true. Moreover, the negation of "if p then q" is logically equivalent to "p and not q."

Exercise. (1) Truth table for $p \vee \sim q \rightarrow \sim p$. (2) Show that $p \vee q \rightarrow r \equiv (p \rightarrow r) \wedge (q \rightarrow r)$. (3) Show that $p \rightarrow q \equiv \sim p \vee q$. (4) Show that $\sim (p \rightarrow q) \equiv p \wedge \sim q$.

1.9.1 Contrapositive Proposition

The *contrapositive* of a conditional proposition of the form "if p then q" is "if $\sim q$ then $\sim p$."

Fact. *A conditional proposition is logically equivalent to its contrapositive.*

1.9.2 Converse and Inverse Propositions

Suppose a conditional proposition of the form "if p then q" is given. Then, the *converse* is "if q then p" and the *inverse* is "if $\sim p$ then $\sim q$."

Fact. *A condtional proposition is not logically equivalent to its converse and to its inverse.*

1.9.3 Biconditional Proposition

Given proposition variable p and q, the *biconditional* of p and q is "p if and only if q." It is true if both p and q have the same truth values and is false if p and q have opposite truth values.

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

1.9.4 Necessary and Sufficient Conditions

If r and s are propositions:

1. r is a *sufficient condition* for s means "if r then s."
2. r is a *necessary condition* for s means "if $\sim r$ then $\sim s$."

Example. Show that r is a necessary condition for s also means "if s then r."

Predicate Logic

2 Propositional Functions

A *propositional function* (or *predicate*) is a sentence that contains a finite variables and becomes a proposition when specific values are substituted for the variables. The *domain* of a propositional function variable is the set of all values that may be substitued in place of the variable.

2.1 Truth Set

If $P(x)$ is a propositional function and x has domain D, the truth set of $P(x)$ is the set of all elements of D that make $P(x)$ true when substituted for x. The truth set of $P(x)$ is denoted$\{x \in D \mid P(x)\}$.

Notation. Suppose $P(x)$ and $Q(x)$ be propositional functions and also suppose the common domain of x is D. The noation $P(x) \Rightarrow Q(x)$ means that every element in the truth set of $P(x)$ is in the truth set of $Q(x)$. The notation $P(x) \Leftrightarrow Q(x)$ means that $P(x)$ and $Q(x)$ have identical truth sets.

3 Quantifiers

One way to obtain proposition from propositional functions is to add quantifiers.

3.1 Universal Quantification

Suppose $Q(x)$ be a propositional function and D the domain of x. A *universal proposition* is a proposition of the form "$\forall x \in D, Q(x)$." The universal proposition is defined to be true if and only if $Q(x)$ is true for every x in D. It is defined to be false if and only if $Q(x)$ is false for at least one x in D. The symbol $\forall$ denotes "for all" and is called the *universal quantifier*.

Note. A value for x for which $Q(x)$ is false is called a *counterexample* to the universal proposition.

3.2 Existential Quantification

Suppose $Q(x)$ be a propositional function and D the domain of x. An *existential proposition* is a proposition of the form "$\exists x \in D$ such that $Q(x)$." The existential proposition is defined to be true if and only if $Q(x)$ is true for at least one x in D. It is false if and only if $Q(x)$ is false for all x in D. The symbole $\exists$ denotes "there exists" and is called the *existential quantifier*.

3.3 Universal Conditional Proposition

One of the most important forms both in mathematics and in computer science is the universal conditional proposition: $\forall x$, if $P(x)$ then $Q(x)$.

Example. As an example, the infomal proposition "if a real number is greater then 2 then its square is greater than 4" can be written formally as $\forall x \in \mathbb{R}$, if $x > 2$ then $x^2 > 4$.

3.3.1 Negation of Universal Proposition

The negation of a proposotion "$\forall x \in D, Q(x)$" is " "$\exists x \in D$ *such that* $\sim Q(x)$."

3.3.2 Negation of Existential Proposition

The negation of the existential proposition "$\exists x \in D$ *such that* $Q(x)$" is "$\forall x \in D$, $\sim Q(x)$."

3.3.3 Negation of Universal Conditional Proposition

The negation of the univeral proposition "$\forall x$, $P(x)$ *then* $Q(x)$" is "$\exists x$ *such that* $P(x)$ *and* $\sim Q(x)$."

4 Methods of Proof

> Mathematics, as a science, commenced when first someone, probably a Greek, proved propositions about "any" things or about "some" things without specification of definite particular things - A. N. Whitehead.

4.1 Definitions

You must clearly understand what the proposition is about to evaluate its truth or falsity. Mathematicians define terms percisely so consider it important to learn definitions virtually word for word.

- An integer n is *even* if and only if $n = 2k$ for some integer k.
- An integer n is *odd* if and only if $n = 2k + 1$ for some integer k.
- An integer n is *prime* if and only if $n > 1$ and for all positive integers r and s, if $n = r.s$, then $r = 1$ or $s = 1$.
- An integer n is *composite* if and only if $n = r \cdot s$ for some positive integers r and s with $r \neq 1$ and $s \neq 1$.
- A real number r is *rational* if and only if $r = a/b$ for some integers a and b with $b \neq 0$. A real number that is not rational is *irrational*.
- If n and d are integers and $d \neq 0$, then n is *divisible by* d if and only if $n = d \cdot k$ for some integer k. Note that the notation $d \mid n$ is read "d divides n."
- Given any integer n and positive integer d, there exist unique integer q and r such that $n = d \cdot q + r$ and $0 \leq r < d$. [The Quotient-Remainder Theorem]
- Given a nonnegative integer n and a positive integer d, n **div** d equals the integer quotient obtained when n is divided by d, and n **mod** d equals the integer remainder obtainded when n is divided by d.
- Given any real number x, the *floor of* x, denoted $\lfloor x \rfloor$, is that unique integer n such that $n \leq x < n + 1$.

- Given any real number x, the *ceiling of x*, denoted $\lceil x \rceil$, is that unique integer n such that $n - 1 < x \leq n$.

4.2 Direct Proof

Prove that if the sum of any two integers is even then so is their difference.

Theorem 2. *$\forall$ integers m and n, if $m + n$ is even then $m - n$ is even.*

Proof. Suppose m and n are integers so that $m + n$ is even. By definition of even, $m + n = 2k$ for some integer k. Subtracting n from both sides gives $m = 2k - n$. So, $m - n = (2k - n) - n = 2k - 2n = 2(k - n)$. But $k - n$ is an integer because it is a difference of integers. Hence, $m - n$ equals 2 times an integer, and so by definition of even, $m - n$ is even. □

Prove that the sum of any two rational numbers is rational.

Theorem 3. *$\forall$ real numbers r and s, if r and s are rational then $r + s$ is rational.*

Proof. Suppose r and s are rational rumbers. Then by definition of rational, $r = a/b$ and $s = c/d$ for some integers a, b, c, and d with $b \neq 0$ and $d \neq 0$. So $r + s = \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$. Let $p = ad + bc$ and $q = bd$. Then p and q are integers because products and sums of integers are integers and because a, b, c, and d are all integers. Thus, $r + s = \frac{p}{q}$ where p and q are integers and $q \neq 0$. So, $r + s$ is rational by definition of a rational number. □

Prove the transitive property of divisibility.

Theorem 4. *$\forall$ integers a, b, and c, if a divides b and b divides c, then a divides c.*

Proof. Suppose a, b, and c are integers such that a divides b and b divides c. By definition of divisibility, $b = a \cdot r$ and $c = b \cdot s$ for some integers r and s. By substitution $c = b \cdot s = (a \cdot r) \cdot s = a \cdot (r \cdot s)$. Let k is an integer since it is a product of integers, and therefore $c = a \cdot k$ where k is an integer. Thus a divides c by definition of divisibility. □

Prove that given any two consecutive integers, one is even and the other is odd.

Theorem 5. *Any two consecutive integers have opposite parity.*

Proof. Suppose that two consecutive integers m and $m + 1$ are given. By the parity property, either m is even or m is odd.

Case 1 (m is even): In this case, $m = 2k$ for some integer k, and so $m + 1 = 2k + 1$, which is odd. Hence, in this case one of m and $m + 1$ is even and the other is odd.

Case 2 (m is odd): In this case, $m = 2k + 1$ for some integer k, and so $m + 1 = (2k + 1) + 1 = 2k + 2 = 2(k + 1)$. But $k + 1$ is an integer because it is a sum of two integers. Therefore,$m + 1$ equals twice some integer, and thus $m+1$ is even. Hence, in this case also one of m and $m+1$ is even and the other is odd.

It follows that regardless of which case actually occurs for the particular m and $m+1$ that are chosen, one of m and $m+1$ is even and the other is odd. □

Modulo 4 Integers Representation

Claim. We say that any integer can be written in one of the four forms: $n = 4q$ or $n = 4q + 1$ or $n = 4q + 2$ or $n = 4q + 3$ for some integer q.

Proof. Given any integer n, apply the quotient-remainder theorem to n with $d = 4$. This implies that there exist an integer quotient q and a remainder r such that $n = 4 \cdot q + r$ and $0 \le r < 4$. But the only nonnegative remainders r that are less than 4 are 0, 1, 2, and 3. Hence, $n = 4q$ or $n = 4q+1$ or $n = 4q+2$ or $n = 4q + 3$ for some integer q. □

The square of any odd integer has the form $8m + 1$ for some integer m.

Theorem 6. *$\forall$odd integers n, $\exists$an integer m such that $n^2 = 8m + 1$.*

Proof. Suppose n is a odd integer. By the quotient-remainder theorem, n can be written in one of the forms: $n = 4q$ or $n = 4q+1$ or $n = 4q+2$ or $n = 4q+3$ for some integer q. In fact, since n is odd and $4q$ and $4q + 2$ are even, n must have one of the forms: $n = 4q + 1$ or $n = 4q + 3$.

Case 1 ($n = 4q + 1$ for some integer q): Since $n = 4q + 3$, $n^2 = (4q + 1)^2 = (4q + 1)(4q + 1) = 16q^2 + 8q + 1 = 8(2q^2 + q) + 1$. Let $m = 2q^2 + q$. Then m is an integer since 2 and q are integers and sums and products of integers are integers. Thus substituting, $n^2 = 8m + 1$where m is an integer.

Case 2 ($n = 4q + 3$ for some integer q): Since $n = 4q + 3$, $n^2 = (4q + 3)^2 = (4q+3)(4q+3) = 16q^2+24q+9 = 16q^2+24q+(8+1) = 8(2q^2+3q+1)+1$. Let $m = 2q^2 + 3q + 1$. Then m is an integer since 2, 3, and q are integers and sums and products of integers are integers. Thus, substituting, $n^2 = 8m + 1$where m is an integer.

Cases 1 and 2 show that given any odd integer, whether of the form $4q + 1$ or $4q + 3$, $n^2 = 8m + 1$ for some integer m. □

Proving a Property of Floor

Theorem 7. *For all real numbers x and all integers m, $\lfloor x + m \rfloor = \lfloor x \rfloor + m$.*

Proof. Suppose a real number x is and an integer m are given. Let $n = \lfloor x \rfloor$. By definition of floor, n is an integer and $n \le x < n + 1$. Add m to all sides to obtain $n + m \le x + m < n + m + 1$. Now $n + m$ is an integer, and so by definition of floor $\lfloor x + m \rfloor = n + m$. But $n = \lfloor x \rfloor$. Hence by substitution $\lfloor x + m \rfloor = \lfloor x \rfloor + m$. □

4.3 Indirect Proof

4.3.1 Argument by Contradiction

Theorem 8. *For all integers n, if $n^2$is odd, then n is odd.*

Proof. Assume, to the contrary, that $\exists$ an integer n such that n^2 is odd and n is even. By definition of even, $n = 2 \cdot k$ for some integer k. So, by substitution $n \cdot n = (2k) \cdot (2k) = 2 \cdot (2 \cdot k \cdot k)$. Let $m = 2 \cdot k \cdot k$. Now m is an integer because products of integers are integers; and 2 and k are integers. Hence, $n^2 = 2 \cdot m$ for some integer m. So, by definition of even $n^2$is even. But this contradicts the supposition that n^2 is odd. □

4.3.2 Argument by Contraposition

Theorem 9. *For all integers n, if n^2 is odd, then n is odd.*

Proof. Form the contrapositive of the given proposition: For all integers n, if n is even, then n^2 is even. Now we'll prove the contrapositive proposition using the method of direct prove. Suppose n is integer. By definition of even $n = 2 \cdot k$ for some integer k. So, by substitution $n \cdot n = (2k) \cdot (2k) = 2 \cdot (2 \cdot k \cdot k)$. Let $m = 2 \cdot k \cdot k$. Now m is an integer because products of integers are integers; and 2 and k are integers. Hence, $n^2 = 2 \cdot m$ for some integer m. So, by definition of even n^2 is even. Hence, the given proposition is true by the logical equivalence between a proposition and its contrapositive. □

Sequences

5 Sequence

Informally, the sequence is a set of elements written in a row. In a sequence $a_m, a_{m+1}, \ldots, a_n$, each element a_k is called a term. The k in a_k is called a subscript or index. A general formula for a sequence is a rule that shows how the values of a_k depend on k.

5.1 Notations

Summation Notation If m and n are integers and $m \leq n$, then the summation from k equals m to n of a_k is the sum of all terms $a_m, a_{m+1}, \ldots, a_n$. We write $\sum_{k=m}^{n} a_k = a_m, a_{m+1}, \ldots, a_n$ and call k the index of the summation, m the lower limit of the summation, and n the upper limit of the summation.

Example. Let $a_1 = -2$, $a_2 = -1$, $a_3 = 0$, $a_4 = 1$, and $a_5 = 2$. Then $\sum_{k=1}^{5} a_k = a_1 + a_2 + a_3 + a_4 + a_5 = (-2) + (-1) + 0 + 1 + 2 = 0$.

We can transform a sum by a change of variable.

Example. Transform the summation $\sum_{k=0}^{6} \frac{1}{k+1}$ by making the specific change of variable: $j = k + 1$.

Product Notation If m and n are integers and $m \leq n$, then the product from k equals m to n of a_k is the product of all terms a_m, a_{m+1}, ... , a_n. We write $\prod_{k=m}^{n} a_k = a_m \cdot a_{m+1} \cdot \ldots \cdot a_n$ and call k the index of the product, m the lower limit of the product, and n the upper limit of the product. For instance, $\prod_{k=1}^{5} k = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120$.

5.2 Properties of Summations and Products

Theorem. *If $a_m, a_{m+1}, a_{m+2}, \ldots$ and $b_m, b_{m+1}, b_{m+2}, \ldots$ are sequences of real numbers and c is any real number, then the following equations hold for any integer $n \geq m$: 1. $\sum_{k=m}^{n} a_k + \sum_{k=m}^{n} b_k = \sum_{k=n}^{n}(a_k + b_k)$ 2. $c \cdot \sum_{k=m}^{n} c \cdot a_k$ 3. $(\prod_{k=m}^{n} a_k) \cdot (\prod_{k=m}^{n} b_k) = \prod_{k=m}^{n} (a_k \cdot b_k)$.*

Example. Using the properties of summation and product, write the following expressions as a single summation or product: (1) $\sum_{k=m}^{n} a_k + 2 \cdot \sum_{k=m}^{n} b_k$ (2) $(\prod_{k=m}^{n} a_k) \cdot (\prod_{k=m}^{n} b_k)$.

5.3 Factorial

Definition. For each positive integer n, the quantity n factorial, denoted $n!$, is defined to be the product of all the integers from 1 to n. That is, $n! = n \cdot (n-1) . (n-2) \cdot \ldots \cdot 3 \cdot 2 \cdot 1$. Zero factorial is defined to be 1. That is, $0! = 1$.

Note. The following formula holds for each positive integer n: $n! = n \cdot (n-1)!$

6 Principle of Mathematical Induction

Let $P(n)$ be a propositional function that is defined for integers n, and let n_0 be a fixed integer. Suppose the following two propositions are true: (1) $P(n_0)$ is true. (2) For all integers$k \geq n_0$, if $P(k)$ is true then $P(k+1)$ is true. Then the proposition for all integers $n \geq n_0$, $P(n)$ is true.

Lemma. *For all integers $n \geq 1$, $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$.*

Proof. The formula is true for $n = 1$: To establish the formula for $n = 1$, we must show that $1 = \frac{1(1+1)}{2} = \frac{2}{2} = 1$, and so the formula is true for $n = 1$.

If the formula is true for $n = k$ then it is true for $n = k + 1$: Suppose $1+2+\ldots+k = \frac{k(k+1)}{2}$, for some integer $k \geq 1$. We must show that $1+2+\ldots+(k+1) = \frac{(k+1)((k+1)+1)}{2}$, or equivalently, that $1+2+\ldots+(k+1) = \frac{(k+1)(k+2)}{2}$.

$1 + 2 + \ldots + (k+1) = 1 + 2 + \ldots + k + (k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{k(k+1)}{2} + \frac{(k+1) \cdot 2}{2} = \frac{(k+1)(k+2)}{2}$. □

Example. Prove that $\sum_{i=0}^{n} r^i = \frac{r^{n+1}-1}{r-1}$, for all integers $n \geq 0$ and all real numbers r except 1.

7 Functions

A function f from a set X to a set Y is a relationship between elements of X and elements of Y with the property that each element of X is related to a unique element of Y. The notation $f : X \rightarrow Y$ means f is a function from X to Y. The set X is called the domain of f and the set Y is called the co-domain of f.

Given an element $x \in X$, there is a unique element $y \in Y$ that is related to x. We can think of x as input and y as the related output. We then say "f sends x to y". The unique element y to which f sends x is denoted $f(x)$ and is called f of x, or the value of f at x, or the image of x under f.

The set of all values of f taken together is called the range of f or the image of X under f. Symbollically: range of $f = \{y \in Y \mid y = f(x)$, for some x in $X\}$. Given an element $y \in Y$, there may exist elements in X with y as their image. The set of all such elements is called the inverse image of y. Symbollically: inverse image of $y = \{x \in X \mid f(x) = y\}$.

Example. Let $X = \{a, b, c\}$ and $Y = \{1, 2, 3, 4\}$. Define a function f from X to Y by specifying that $f(a) = 2$, $f(b) = 4$, and $f(c) = 2$. Then, domain of $f = \{a, b, c\}$, co-domain of $f = \{1, 2, 3, 4\}$, range of $f = \{2, 4\}$, inverse image of $2 = \{a, c\}$, inverse image of $4 = \{b\}$, inverse image of $1 = \emptyset$ and we can represent f as a set of ordered pairs: $\{(a, 2), (b, 4), (c, 2)\}$.

7.1 Injective or One-to-One Functions

Let F be a function from a set X to a set Y. F is one-to-one if, and only if, for all elements x_1 and x_2 in X, if $F(x_1) = F(x_2)$, then $x_1 = x_2$. Or equivalently, if $x_1 \neq x_2$, then $F(x_1) \neq F(x_2)$.

Let F be a function from a set X to a set Y. F is *not* one-to-one if, and only if, $\exists$ elements x_1 and x_2 in X with $F(x_1) = F(x_2)$ and $x_1 \neq x_2$.

Example. Let $X = \{1, 2, 3\}$and $Y = \{a, b, c, d\}$. Define $H : X \rightarrow Y$ by specifying that $H(1) = c$, $H(2) = a$, and $H(3) = d$. Define $K : X \rightarrow Y$ by specifying that $K(1) = d$, $K(2) = b$, and $K(3) = d$. Then, H is one-to-one because each of the three elements of domain of H is sent by H to a different element of the co-domain: $H(1) \neq H(2)$, $H(1) \neq H(3)$, and $H(2) \neq H(3)$. However, K is not one-to-one because $K(1) = K(3) = d$ but $1 \neq 3$.

Lemma. *If the function $f : \mathbb{R} \rightarrow \mathbb{R}$ is defined by the rule f(x)=4x-1, for all real numbers x, then f is one-to-one*

Proof. Suppose x_1 and x_2 are real numbers such that $f(x_1) = f(x_2)$.Then, $4x_1 - 1 = 4x_2 - 1$, Adding 1 to both sides gives $4x_1 = 4x_2$, and dividing both sides by 4 gives $x_1 = x_2$, which is required. □

Lemma. *If the function $g : \mathbb{Z} \rightarrow \mathbb{Z}$ is defined by the rule $g(n) = n^2$, for all $n \in \mathbb{Z}$, then g is not one-to-one.*

Proof. (by counterexample) Let $n_1 = 2$ and $n_2 = -2$. Then $g(n_1) = g(2) = 2^2 = 4$ and also $g(n_2) = g(-2) = (-2)^2 = 4$. Hence, $g(n_1) = g(n_2)$ but $n_1 \neq n_2$, and so g is not one-to-one function. □

7.2 Surjective or Onto Functions

Let F be a function from a set X to a set Y. F is onto if, and only if, given any element y in Y it is possible to find an element x in X with the property that y=F(x).

Let F be a function from a set X to a set Y. F is not onto if, and only if, $\exists y$ in Y such that $\forall x \in X$, $F(x) \neq y$.

Example. Let $X = \{1, 2, 3, 4\}$and $Y = \{a, b, c\}$. Define $H : X \to Y$ by specifying that $H(1) = c$, $H(2) = a$, $H(3) = c$, and $H(4) = b$. Define $K : X \to Y$ by specifying that $K(1) = c$, $K(2) = b$, and $K(4) = c$. Then, H is onto because each of the three elements of the co-domain of H is the image of some element of the domain of H: $a = H(2)$, $b = H(4)$, and $c = H(1) = H(3)$. However, K is not onto because $a \neq K(x)$ for any x in $\{1, 2, 3, 4\}$.

Lemma. *If $f : \mathbb{R} \to \mathbb{R}$ is the function defined by the rule $f(x) = 4x - 1$ for all real numbers x, then f is onto.*

Proof. Let $y \in \mathbb{R}$. Let $x = \frac{y+1}{4}$. Then x is a real number since sums and quotients (other than by 0) of real numbers are real numbers. It follows that $f(x) = f\left(\frac{y+1}{4}\right) = 4 \cdot \left(\frac{y+1}{4}\right) - 1 = (y + 1) - 1 = y$. □

Lemma. *If the function $h : \mathbb{Z} \to \mathbb{Z}$ is defined by the rule $h(n) = 4n - 1$ for all integers n, then h is not onto.*

Proof. (by counterexample) The co-domain of h is $\mathbb{Z}$ and $0 \in \mathbb{Z}$. But $h(n) \neq 0$ for any integer n. For if $h(n) = 0$, then $4n - 1 = 0$ by definition of h, which is $4n - 1$ or $n = \frac{1}{4}$. But $\frac{1}{4}$ is not an integer. Hence, there is no integer n for which $f(n) = 0$, and so f is not onto. □

7.3 Bijection or one-to-one correspoundence

A bijection from a set X to a set Y is a function $F : X \to Y$ that is both one-to-one and onto.

7.4 Inverse Function

Suppose $F : X \to Y$ is a bijection; that is, suppose F is one-to-one and onto. Then there is a function $F^{-1} : Y \to X$ that is defined as follows: Given any element y in Y, $F^{-1}(y)$ is that unique element x in X such that $F(x)$ equals y. The function F^{-1} is called the inverse function of F.

Example. The function $f : \mathbb{R} \to \mathbb{R}$ defined by the formula $f(x) = 4x - 1$ for all real numbers x. Then by definition of f^{-1}, $f^{-1}(y) =$ that unique real number y such that $f(x) = y$. But $f(x) = y \Leftrightarrow 4x - 1 = y \Leftrightarrow x = \frac{y+1}{4}$. Hence, $f^{-1}(y) = \frac{y+1}{4}$, which is the inverse function of the given function $f(x) = 4x - 1$.

Lemma. *If X and Y are sets and $F : X \rightarrow Y$ is bijection (that is, one-to-one and onto), then $F^{-1} : Y \rightarrow Y$ is also bijection.*

Proof. F^{-1} is one-to-one: Suppose y_1 and y_2 are elements of Y such that $F^{-1}(y_1) = F^{-1}(y_2)$. Let $x = F^{-1}(y_1) = F^{-1}(y_2)$. Then, $x \in X$, and by definition of F^{-1}, $F(x) = y_1$ since $x = F^{-1}(y_1)$ and $F(x) = y_2$ since $x = F^{-1}(y_2)$. Consequently, $y_1 = y_2$ since each is equal to $F(x)$.

F^{-1} is onto: Suppose $x \in X$. Let $y = F(x)$. Then $y \in Y$, and by definition of F^{-1}, $F^{-1}(y) = x$. □

7.5 Pigeonhole Principle

A function from one finite set to a smaller finite set cannot be one-to-one: There must be at least two elements in the domain that have the same image in the co-domian.

Example. A group of thirteen people must contain at least two who were born in the same month, for there are only twelve months in a year and $13 > 12$.

The truth of the pigeonhole principle depends on the sets being finite. So, the definitions of finite and infinite sets are as follows:

Definition. A set is called finite if, and only if, it is the empty set or there is a one-to-one correspondence from $\{1, 2, \ldots, n\}$ to it, where n is a positive integer. In the first case, the number of elements in the set is said to be 0, and in the second case it is said to be n. A set that is not finite is called infinite.

Lemma. *For any funtion f from a finite set X to a finite set Y, if $n(X) > n(Y)$, then f is not one-to-one.*

Proof. Suppose f is any function from a finite set X to a finite set Y where $n(X) > n(Y)$. Let $n(Y) = m$, and denote the elements of Y by $y_1, y_2, \ldots, y_m$. Recall that for each y_i in Y, the inverse image set $f^{-1}(y_i) = \{x \in X : f(x) = y_i\}$. Now consider the collection of all the inverse image sets for all the elements of Y: $f^{-1}(y_1), f^{-1}(y_2), \ldots, f^{-1}(y_m)$. By definition of function, each element of X is sent by f to some element of Y. Hence, each element of X is one of the inverse image sets, and so the union of all these sets equals X. But also by definition of function, no element of X is sent by f to more than one element of Y. Thus each element of X is in only one of the inverse image sets, and so the inverse image sets are mutually disjoint. Therefore, by the addition rule, $n(X) = n(f^{-1}(y_1)) + n(f^{-1}(y_2)) + \ldots + n(f^{-1}(y_m))$ (Equation 1).

Now suppose that f is one-to-one. Then, each set $f^{-1}(y_i)$ has at most one element, and so $n(f^{-1}(y_1)) + n(f^{-1}(y_2)) + \ldots + n(f^{-1}(y_m)) \leq 1 + 1 + \ldots + 1 = m$ (Equation 2).

Putting Equation 1 and Equation 2 togather gives that $n(X) \leq m = n(Y)$. This contradicts the fact that $n(X) > n(Y)$, and so the supposition that f is one-to-one must be false. Hence, f is not one-to-one. □

7.6 Composition of Functions

Let $f : X \to Y'$ and $g : Y \to Z$ be functions with the property that the range of f is a subset of the domain of g. Define a new function $g \circ f : X \to Z$ as follows: $(g \circ f)(x) = g(f(x))$ for all $x \in X$. The function $g \circ f$ is called the composition of f and g.

Example. Let $f : \mathbb{Z} \to \mathbb{Z}$ be the successor function and let $g : \mathbb{Z} \to \mathbb{Z}$ be the squaring function. Then $f(n) = n + 1$ for all $n \in \mathbb{Z}$ and $g(n) = n^2$ for all $n \in \mathbb{Z}$. The function $g \circ f$ and $f \circ g$ are defined as follows: $(g \circ f)(n) = g(f(n)) = g(n+1) = (n+1)^2$ for all $n \in \mathbb{Z}$, and $(f \circ g) = f(g(n)) = f(n^2) = n^2 + 1$ for all $n \in \mathbb{Z}$.

Two functions from one set to another are equal if, and only if, they take the same values. In this case, $(g \circ f)(1) = (1+1)^2 = 4$, whereas $(f \circ g)(1) = 1^2+1 = 2$. Thus, the two functions $g \circ f$ and $f \circ g$ are not equal: $g \circ f \neq f \circ g$.

The above example illustrates the important fact that composition of functions is not a commutative operation: for general functions F and G, $F \circ G$ need not necessarily equal $G \circ F$, although the two may be equal.

Exercise. Let $X = \{1, 2, 3\}$, $Y' = \{a, b, c, d\}$, $Y = \{a, b, c, d, e\}$, $Z = \{x, y, z\}$. Define functions $f : X \to Y'$ and $g : Y \to Z$ as $f(1) = c$, $f(2) = b$, $f(3) = a$, and $g(a) = y$, $g(b) = y$, $g(c) = z$, $g(d) = z$, and $g(e) = z$. Find the arrow diagram for $g \circ f$ and find the range of $g \circ f$.

Lemma. *If $f : X \to Y$ and $g : Y \to Z$ are both one-to-one functions, then $g \circ f$ is one-to-one.*

Proof. Suppose $f : X \to Y$ and $g : Y \to Z$ are both one-to-one functions. Suppose x_1 and x_2 are elements of X such that $(g \circ f)(x_1) = (g \circ f)(x_2)$. By definition of composition of functions, $g(f(x_1)) = g(f(x_2))$. Since g is one-to-one, $f(x_1) = f(x_2)$. And since f is one-to-one, $x_1 = x_2$. □

Lemma. *If $f : X \to Y$ and $g : Y \to Z$ are both onto functions, then $g \circ f$ is onto.*

Proof. Suppose $f : X \to Y$ and $g : Y \to Z$ are both onto functions. Let z be a element of Z. Since g is onto, there is an element y in Y such that $g(y) = z$. And since f is onto, there is an element x in X such that $f(x) = y$. Hence, there exists an element x in X such that $(g \circ f)(x) = g(f(x)) = g(y) = z$. It follows that $g \circ f$ is onto. □

8 Recursion

A recurrence relation for a sequence $a_1, a_2, a_3, \ldots$ is a formula that relates each term a_k to certain of its predecessors $a_{k-1}, a_{k-2}, \ldots, a_{k-i}$, where i is a fixed integer and k is any integer greater than or equal to i. The initial conditions for such a recurrence relation specify the values of $a_0, a_1, a_2, \ldots, a_{i-1}$.

For example, a sequence $b_0, b_1, b_2, \dots$ can be defined recursively as follows: For all integer $k \geq 2$, $b_k = b_{k-1} + b_{k-2}$ (recurrence relation) and $b_0 = 1$, $b_1 = 3$ (initial conditions). Since b_0 and b_1 are given, b_2 can be computed using recurrence relation. $b_2 = b_1 + b_0 = 3 + 1 = 4$. Then, since both b_1 and b_2 are now known, b_3 can be computed using recurrence relation. $b_3 = b_2 + b_1 = 4 + 3 = 7$. In general, the recurrence relation says that any term of the sequence after b is the sum of the two preceding terms. Thus, $b_4 = b_3 + b_2 = 7 + 4 = 11, b_5 = b_4 + b_3 = 11 + 7 = 18$, and so forth.

8.1 Iteration Method

An explicit formula for the sequence, whose recurrence relation and initial conditions are given, is called a solution to the recurrence relation. The basic method for finding an explicit formula (i.e., solution) for a recursively defined sequence is iteration. The following example shows the working of the meothod of iteration.

let $a_0, a_1, a_2, \dots$ be the sequence defined recursively as follows: For all integers $k \geq 1$, $a_k = a_{k-1} + 2$ (recurrence relation) $a_0 = 1$ (initial condition). We use iteration to guess an explicit formula for the sequence.

Recall that to say $a_k = a_{k-1} + 2$ for all integers $k \geq 1$ means no matter what positive integer is replaced k. In particular, $a_1 = a_0 + 2, a_2 = a_1 + 2, a_3 = a_2 + 2$, and so forth. Now use the initial condition to begin a process of successive substitutions into these equations, not just of numbers but of numerical expressions. Here's how the process works for the given sequence:

$a_0 = 1$
$a_1 = a_0 + 2 = 1 + 2$
$a_2 = a_1 + 2 = (1 + 2) + 2 \qquad = 1 + 2 + 2$
$a_3 = a_2 + 2 = (1 + 2 + 2) + 2 \qquad = 1 + 2 + 2 + 2$
$a_4 = a_3 + 2 = (1 + 2 + 2 + 2) + 2 = 1 + 2 + 2 + 2 + 2$

We use the shorthand $k \cdot 2$ in place of $2 + 2 + \dots + 2$ (k items), so starting from a_0.

$a_0 = 1 \qquad = 1 + 0 \cdot 2$
$a_1 = a_0 + 2 = 1 + 2 \qquad = 1 + 1 \cdot 2$
$a_2 = a_1 + 2 = (1 + 2) + 2 = 1 + 2 + 2 \qquad = 1 + 2 \cdot 2$
$a_3 = a_2 + 2 = (1 + 2 + 2) + 2 = 1 + 2 + 2 + 2 \qquad = 1 + 3 \cdot 2$
$a_4 = a_3 + 2 = (1 + 2 + 2 + 2) + 2 = 1 + 2 + 2 + 2 + 2 \qquad = 1 + 4 \cdot 2$
$a_5 = a_4 + 2 = (1 + 2 + 2 + 2 + 2) + 2 = 1 + 2 + 2 + 2 + 2 + 2 \qquad = 1 + 5 \cdot 2$

So the guess is:

$$a_n = 1 + n \cdot 2 = 1 + 2n$$

The answer obtained for this problem is just a guess. To be sure of the correctness of this guess, you will need to check it by mathematical induction.

The sequence like the one in the above example, in which each term equals the previous term plus a fixed constant, is called an *arithmetic sequence*.

Definition. A sequence $a_0, a_1, a_2, \dots$ is called an *arithmetic sequence* if and only if there is a constant d such that $a_k = a_{k-1} + d$ for all integers $k \geq 1$. Or equivalently, $a_n = a_0 + d \cdot n$ for all integers $n \geq 0$.

In a geometric sequence, each term equals the previous term times a fixed constant.

Definition. A sequence $a_0, a_1, a_2, \ldots$ is called a *geometric sequence* if and only if there is a constant r such that $a_k = r \cdot a_{k-1}$ for all integers $k \geq 1$. Or equivalently, $a_n = a_0 \cdot r^n$ for all integers $n \geq 0$.

Exercise. Let r be a fixed nonzero constant and suppose a sequence $a_0, a_1, a_2, \ldots$ is defined recursively as follows: $a_k = r \cdot a_{k-1}$ for all integers $k \geq 1$, $a_0 = a$. Use iteration to guess an explicit formula for this sequence.

9 Relations

Let A and B be sets. A (binary) relation R from A to B is a subset $A \times B$. Given an ordered pair (x, y) in $A \times B$, x is related to y by R, written xRy, if and only if (x, y) is in R.

For instance, let $A = \{0, 1, 2\}$ and $B = \{1, 2, 3\}$. Let us say that an element x in A is related to an element y in B if and only if x is less than y. Then $0R1$ since $0 < 1$, $0R2$ since $0 < 2$, $0R3$ since $0 < 3$, $1R2$ since $1 < 2$, $1R3$ since $1 < 3$, and $2R3$ since $2 < 3$. Recall that the Cartesian product of A and B, $A \times B$, consists of all ordered pairs whose first element is in A and whose second element is in B: $A \times B = \{(x, y) : x \in A \wedge y \in B\}$. In this case, $A \times B = \{(0, 1), (0, 2), (0, 3), (1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3)\}$. The elements of some ordered pairs in $A \times B$ are related while the elements of other ordered pairs are not. Consider the set of all ordered pairs in $A \times B$ whose elements are related: $\{(0, 1), (0, 2), (0, 3), (1, 2), (1, 3), (2, 3)\}$. Observe that knowing which ordered pairs lie in this set is equivalent to knowing which elements are related to which.

Example. Let $A = \{1, 2\}$ and $B = \{1, 2, 3\}$ and define a binary relation R from A to B as follows: given any (x,y)$\in A \times B$, (x,y)$\in R$ if and only if x−y is even. Then $A \times B = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3)\}$. To determine explicitly the composition of R, examine each ordered pair in $A \times B$ to see whether its elements satisfy the defining condition of R. $(1, 1) \in R$ because $1 - 1 = 0$ and 0 is even, $(1, 2) \notin R$ because $1 - 2 = -1$ and -1 is not even, $(1, 3) \in R$ because $1 - 3 = 2$ and -2 is even, $(2, 1) \notin R$ because $2 - 1 = 1$ and 1 is not even, $(2, 2) \in R$ because $2 - 2 = 0$ and 0 is even, and $(2, 3) \notin R$ because $2 - 3 = -1$ and -1 is not even. Thus, $R = \{(1, 1), (1, 3), (2, 2)\}$.

Generalize the relation in the above example to the set of all integers $\mathbb{Z}$. That is, define a binary relation E from $\mathbb{Z}$ to $\mathbb{Z}$ as follows: for all $(m, n) \in \mathbb{Z} \times \mathbb{Z}$, mEn if and only if $m - n$ is even. Then, $4E0$ because $4 - 0 = 4$ and 4 is even ... and so forth. Now we'll show that if n is odd then we have $nE1$.

Lemma. *If n is any odd integer, then $nE1$.*

Proof. Suppose n is nay odd integer. Then $n = 2k + 1$ for some integer k. Now by definition of E, $nE1$ if and only if $n - 1$ is even. But by substitution, $n-1 = (2k+1)-1 = 2$k, and since k is an integer, $2k$ is even. Hence $nE1$. □

Exercise. Define a binary relation C from $\mathbb{R}$ to $\mathbb{R}$ as follows: for any $(x, y) \in \mathbb{R} \times \mathbb{R}, (x, y) \in C$ if and only if $x^2 + y^2 = 1$.

9.1 Functions

A function F from a set A to a set B is a relation from A to B that satisfies the following two properties: (1) For every element x in A, there is an element y in B such that $(x, y) \in F$. (2) For all elements x in A and y and z in B, if $(x, y) \in F$ and $(x, z) \in F$, then $y = z$. If F is a function from A to B, we write $y = F(x)$ if and only if $(x, y) \in F$.

Example. Let $A = \{2, 4, 6\}$ and $B = \{1, 3, 5\}$. The relations R define as $R = \{(2, 5), (4, 1), (4, 3), (6, 5)\}$ and the relation S define as for all $(x, y) \in A \times B, (x, y) \in S$ if and only if $y = x + 1$. Then, the relation R is not a function because it does not satisfy property (2). The ordered pairs $(4, 1)$ and $(4, 3)$ have the same first element but different second elements. The relation S is not a function because it does not satisfy property (1). It is not true that every element of A is the first element of an ordered pair in S. For example, $6 \in A$ but there is no y in B such that $y = 6 + 1 = 7$.

Exercise. (a) Define a relation from $\mathbb{R}$ to $\mathbb{R}$ as follows: for all $(x, y) \in \mathbb{R} \times \mathbb{R}, (x, y) \in C$ if and only if $x^2 + y^2 = 1$. (b) Define a relation from $\mathbb{R}$ to $\mathbb{R}$ as follows: for all $(x, y) \in \mathbb{R} \times \mathbb{R}, (x, y) \in L$ if and only if $y = x - 1$. Which one C or L is a function?

9.2 Inverse Relation

Let R be a relation from A to B. Define the inverse relation R^{-1} from B to A as follows: $R^{-1} = \{(y, x) \in B \times A : (x, y) \in R\}$.

References

[1] Kenneth A. Ross and Charles R. B. Wright, Discrete Mathematics, 5th Edition, Pearson Education Inc., 2003.

[2] Susanna S. Epp, Discrete Mathematics with Applications, PWS Publishing Company, Boston, MA, 1995

[3] .Seymour Lipschutz and Marc Lipson, Schaum's Outline of Theory and Problems of Discrete Mathematics, McGraw-Hill, 1997.