Course Notes for CS336: Preliminary Material

Jayadev Misra
The University of Texas at Austin

July 2001

Contents

1 Introduction

1. Introduce self, TA.
2. Go over the handout.
3. What is this course about?
4. No programming.
5. Why is this material is useful?
6. How to study for it?
7. How I teach?

2 Preliminary Material

Reading Assignment, Homework Read Rosen 1.4, 1.5, 1.6
Homeworks:
1.4: 7, 8, 10, 13, 15, 22, 25
1.5: 35, 37, 40, 44
1.6: 24, 26, 27, 35, 38

2.1 Sets

2.1.1 Set Enumeration, Comprehension

$\{cat, dog, pig\}$, $\{3, 5, 7\}$, $\{0, 1, 2, ...\}$.
Order is unimportant.
Repetition is irrelevant.
We restrict our set elements to mathematical objects.
Element types could be mixed: $\{3, \{3, 5\}, 7\}$
Set equality: Note that $3 \neq \{3\}$.

- Definition through *Enumeration*:

  Roman Alphabet, Arabic Numerals, Pascal Keywords.

- Definition through *Comprehension*: $\{x|$ conditions on $x\}$.

  All integers between 0 and 10: $\{x|\ 0 \leq x \leq 10\}$.

  All even integers between 0 and 10: $\{x|\ 0 \leq x \leq 10\ \wedge$ even $x\}$, or explicitly $\{0, 2, 4, 6, 8, 10\}$.

  All even integers: $\{x|$ even $x\}$. Infinite set.

  All integers that are even and odd: $\{x|$ even $x\ \wedge$ odd $x\}$.

Some important sets: integers , naturals, positive integers, negative integers, reals, rationals.

Empty set: written as ϕ. Note $\phi \neq \{\phi\}$.

Set membership written as $x \in S$.

$3 \in \{3, \{3, 5\}, 7\}$.
$\{3, 5\} \in \{3, \{3, 5\}, 7\}$.

Cardinality of S, written as $|S|$:

$|\{2\}| = 1$, $|\phi| = 0$, $|\{x | \ 0 \leq x \leq 10\}| = 11$
What is the cardinality of naturals?

Subset

naturals $\subseteq$ integers,
$\phi \subseteq S$, $S \subseteq S$,
$S \subseteq T, T \subseteq S \ \Rightarrow \ S = T$
$S \subseteq T, T \subseteq U \ \Rightarrow \ S \subseteq U$
$S \subseteq T$, S, T finite $\Rightarrow$ cardinality of $S \leq$ cardinality of T.

Powerset Powerset of S is the set of all subsets of S.

For $S = \{0, 1, 2\}$, the powerset is,

$$\{\{\}, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}, \{1, 2\}, \{0, 1, 2\}\}.$$

What is the powerset ϕ? $\{\{\}\}$.
The cardinality of the powerset of S is $2^{|S|}$. Check for ϕ.
Show the connection between subsets and n-bit strings.

2.1.2 Operations on Sets

- **Union** Compute $S \cup T$ where

  $S = \{0, 1, 2\}$ and $T = \{3, 4\}$,
  $S = \{0, 1, 2\}$ and $T = \{2, 3, 4\}$,
  $S = \{0, 1, 2\}$ and $T = \{0\}$.

  $N \cup Z = Z$, $S \cup \phi = S$, $S \cup S = S$.

  $\cup$ is not quite like the plus on integers; you can't cancel:
  $S \cup T = T$ does not mean that $S = \phi$.
  Formally, $x \in S \cup T$ means $x \in S$ or $x \in T$.

  Note: $S \subseteq T \ \Rightarrow \ S \cup T = T$.

- **Intersection** Compute $S \cap T$ where

  $S = \{0, 1, 2\}$ and $T = \{2, 3, 4\}$,
  $S = \{0, 1, 2\}$ and $T = \{0\}$,
  $S = \{0, 1, 2\}$ and $T = \{3, 4\}$.

$S \cap \phi = \phi$, $S \cap S = S$.
Formally, $x \in S \cap T$ means $x \in S$ and $x \in T$.

Note:

$S \cap T \subseteq S \subseteq S \cup T$.
$S \subseteq T \;\Rightarrow\; S \cap T = S$.

Two sets are *disjoint* if their intersection is empty; i.e., they have no common element.

- **Difference** $S - T = \{x | \; x \in S \wedge \; x \notin T\}$.

  $\{2, 3\} - \{1, 2\} = \{3\}$.

  $\{2, 3\} - \{1, 0\} = \{2, 3\}$.

  Compute: $((\{0, 1, 2\} \cup \{1, 3, 4\}) - \{3\}) \cap \{1, 2, 3\}$. Answer is $\{1, 2\}$.

  Note: $S - \phi = S$, $S \subseteq T \;\Rightarrow\; S - T = \phi$.

  Note: $S - T$ may be different from $T - S$.

- **Complement**

  Given a universal set $\overline{S}$ is the set of elements not in S. Let integers be the universal set; then $\overline{evens} = odd$.

- **Facts about set operations**

Binary Operators

Commutative: +, $\times$, min, max, xor(addition mod 2), lowest-common-ancestor of a pair of nodes in a tree.

Operators that are not commutative: subtraction, division

Associative: +, $\times$, min, max, xor(addition mod 2), String Concatenation, Matrix Product; Function Composition; ";" in C++, lowest-common-ancestor of a pair of nodes in a tree.

Note: No paranthesis needed when writing a chain of associative operations.

Operators that are not associative: subtraction.

Operators that are commutative but not associative:
$x \oplus y = (x + y)/2$. Note that $\oplus$ is commutative.
$(0 \oplus 4) \oplus 2 = 2 \oplus 2 = 2$, $0 \oplus (4 \oplus 2) = 0 \oplus 3 = 1.5$.

Operators that are not commutative but associative: string concatenation, Matrix product, Function Composition.

$\cup$, $\cap$ are commutative and associative.
$S \cap \overline{S} = \phi$, $S \cup \overline{S} = U$.
$S \cup (T \cap R) = (S \cup T) \cap (S \cup R)$,
$S \cap (T \cup R) = (S \cap T) \cup (S \cap R)$,
Contrast with $a \times (b + c)$.

Mention Venn diagrams.

- **Cartesian Products**

  Ordered pairs: (name, telephone)

  Tuples, n-tuples.

  Note: tuples are different from sets; order matters and the same element may appear several times in a tuple.

  $S \times T = \{(x, y) | \; x \in S \; \wedge \; y \in T\}$.
  $\{0, 1\} \times \{1\} = \{(0, 1), (1, 1)\}$.
  $\{0, 1\} \times \{2, 3\}$?

  Cartesian product is not commutative. $S \times T$ may be different from $T \times S$.

  Cartesian product is associative.

  Compute $\{0, 1\} \times \{1, 2\} \times \{2, 0\}$.

  Given finite sets S, T, $|S \times T| = |S| \times |T|$.

  Cartesian product can be shown as a matrix.

2.2 Function

A mapping from S to T. Either or both of S, T may be infinite. We write $f : S \longrightarrow T$ for a function with domain S and range (or codomain) T.
Example: ha : {ant, cow, cat, pig, dog} $\longrightarrow$ {T, F}.
ha(ant) = T, ha(cow) = F, ha(cat) = T, ha(pig) = F, ha(dog) = F.
Note: Every point in the domain maps to some point in the range.

1. Onto/surjective: covers the whole range. Note that ha is onto.

2. one-to-one/injective: each element in the range is mapped to by at most one element. $f(x) = f(y) \Rightarrow x = y$. ha is not one-to-one.

3. one-to-one and onto (or, bijective): both properties.

Let S be some set and id is the identity function. Show it is bijective.
Let $S = \{0, 1, 2\}$. Let $f : S \longrightarrow S$ where $f(x) = x+1 \bmod 3$. Then f is bijective.
Let f be the successor function on the set of naturals. Is f bijective?
Let $f : R \longrightarrow Z$, where $f(x)$ is the largest integer not exceeding x. Is f onto?

Show a function that is one-to-one but not onto.
Show a function that is onto but not one-to-one.
Show a function that is both.
Show a function that is neither.
Show a mapping that is not a function.
Given that $f : S \longrightarrow T$, what is the relationship between $|S|$ and $|T|$? What if f is onto, one-to-one or bijective?

Function Composition $(f \circ g)(x)$ is $f(g(x))$. Thus, $f \circ g$ is a function provided $g : R \longrightarrow S$ and $f : S \longrightarrow T$. Then, $f \circ g : R \longrightarrow T$. Similarly define $f \circ g \circ h$. Often we write fg in place of $f \circ g$.

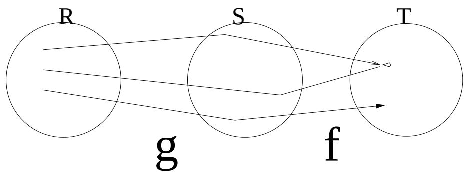

Figure 1: Compositions of f, g

Given $f : S \longrightarrow S$, write f^2 for $f \circ f$.

Let $S = \{0, 1, 2\}$. Let $f : S \longrightarrow S$ where $f(x) = x + 1 \bmod 3$.
What is $f^2,\ f^3$?

Function composition is associative but not commutative.

Problem (Very Hard): f is a function from naturals to naturals. Suppose $f^2(n) < f(n+1)$, for all naturals n. show that f is the identity function.

Function Inverse For a bijective function f, there is a function g, such that $fg = \text{id}$. That is if $f(a) = b$ then $g(b) = a$. We say g is the inverse of f, and write f^{-1} for g. The inverse of f is written as f^{-1}.

1. $ff^{-1} = f^{-1}f = \text{id}$
2. $f^{-1^{-1}} = f$
3. $(fg)^{-1} = g^{-1}f^{-1}$

Suppose every person has a single wife, then does every woman have a (single) husband?

Why does f not have an inverse if it is not bijective?

2.3 Relation

Reading Assignment, Homework Read Rosen: 6.1, 6.5, 6.6
Home work:

Graph of a function: Consider the following function,

$$f : \{0, 1, 2, 3, 4\} \longrightarrow \{0, 1, 2, 3, 4\}; \text{ where } f(x) = x^2 \bmod 5.$$

We can depict the function by the following graph.

In this picture there is exactly one outgoing arrow from each node. (Note that not all nodes have incoming arrows, and some have more than one incoming arrow). Relation

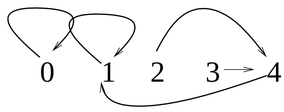

Figure 2: Graph of a Function

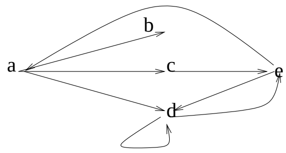

Figure 3: Graph of a Relation

is a generalization of function; there are multiple or zero incoming/outgoing arrows to/from a node.

The arrows in Figure 3 can be represented by

$$\{(a,b),(a,c),(a,d),(c,e),(d,d),(d,e),(e,a),(e,d)\}.$$

This is a subset of $\{a,b,c,d,e\} \times \{a,b,c,d,e\}$.

In general, a relation is a subset of $S \times T$; such a relation is called a relation from S to T. A binary relation over S is a subset of $S \times S$. Here is an example of a more general relation.

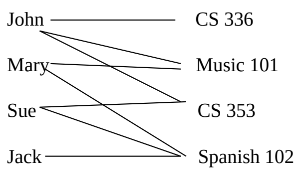

Figure 4: A general relation

Suppose you are given some facts about who knows who in USA. How many intermediate persons are in the chain between you and Bill Gates?

Depict the “knows” in a picture.

Given two items either the relation holds or does not hold between them. Its result is a boolean. $\cup$ is not a relation.

Some common relations:

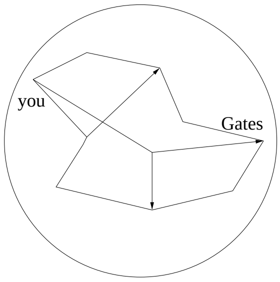

Figure 5: "knows" Relation

S	T	Name of Relation	Example
People	People	knows	Misra knows Gates
People	People	Brother	John is Jack's brother
People	things	owns	John owns a Ford
People	Tel. No.	has	Misra has 471-9550

Mathematical Examples: $\leq, <, =, \neq, >, \geq$ on reals.
divides on integers
$equals \pmod 3$ over integers
substring over strings
member over elements and sets.

Every function is a relation: $f : S \longrightarrow T$ is the subset $\{(x, F(x)) | \; x \in S\}$ of $s \times T$. Not every relation is a function.

For binary relations, we write them in infix style:
$3 < 5$, $1 \in \{1, 2\}$, etc. In prolog you may write $knows$(Misra, Bill).

Upper and lower bounds: b is an upper bound of x, y if $x \leq b$ and $y \leq b$.
Least upper bound, greatest lower bound: c is a least upper bound of x, y if it is an upper bound and it is the smallest such, i.e., for any upper bound b of x, y, $c \leq b$.

The least upper bound may not always exist. If $x \leq b$ means that b is an ancestor of x then for siblings x, y, both father and mother are least upper bounds.

Show that if a least upper bound exists, it is unique.

Special kinds of relations

- Reflexive: $x \leq x$, x divides x, s substring s, $p \subseteq p$, $p \Rightarrow p$, $x = x$, s rotation s.

  Not reflexive: brother, $<$, $\in$, $\neq$.

- Symmetric: brother relation over boys, $=$, $\neq$, $\equiv$, disjoint (sets x, y are disjoint if $x \cap y = \phi$), $equals \pmod 3$.

  Not symmetric: brother relation over siblings, $\Rightarrow$, substring, divides, $\leq$.

- Transitive: $\leq, <, =, >, \geq$ on reals, $\subseteq$, $\Rightarrow$, divides, $equals \pmod 3$.

  Is "sibling" transitive? No.

  Not transitive: "father of", $x = y + 1$, knows, $\neq$.

  Exercise: Show relations that are
  reflexive, symmetric but not transitive
  reflexive, transitive but not symmetric
  symmetric, transitive but not reflexive.

  Solution to the last problem: Over the set of integers define xRy by $x \times y$ is odd. The relation is symmetric because, $xRy \ \equiv$ both x and y are odd. It is transitive, by the same argument. However zRz does not hold if z is even.

- Equivalence: Reflexive, symmetric and transitive:

$$=, \equiv, \ equals \pmod 3, \text{rotation.}$$

Problem: Let f be a string of length N. It is required to decide if all cyclic rotations of f are distinct, i.e., check if $(\forall i, j : 0 \leq i < N,\ 0 \leq j < N,\ i \neq j : f.i \neq f.j)$, where $f.i$ is the left rotation of f by i positions. (see /Notes.dir/CyclicEquivalence.tex).

We can depict a binary relation pictorially by a graph. What is the structure of the graph if the relation is reflexive, symmetric or transitive?

What is the structure of the graph if the relation is an equivalence relation?

Example: x is a *fellow-of* y if they are citizens of the same country. This partitions the set of people.

Places that are in the same time zone. How many partitions? Thus, we can store this more efficiently:

GMT: London, Greenwich, ...
GMT+1: Amsterdam, Frankfurt, Brussels ..
GMT-6: Austin, Dallas, Chicago, ...

Connectivity: Road network after a typhoon, Computer network after a global crash.

Infinite number of equivalence classes: $x \sim y$ for strings x, y if they have the same number of 1's.
0 1's: 0, 00, 000, 0000, ...
1 1's: 1, 01, 001, 10, 100, 1000, .., 00100, ...
2 1's: 11, 101, 110, ...

Equivalence relation over infinite binary strings: For infinite binary strings x and y write $x \sim y$ if x and y differ only in a finite number of corresponding positions (i.e., $x_i = y_i$, for almost all i). Show that $\sim$ is an equivalence relation. Is the number of equivalence classes finite or infinite?

Solution to the Second Part: The number of equivalence classes is infinite. Let z^i be the string which has 2^i zeroes followed by 2^i ones. Then z^i and z^j, where $i \neq j$, differ in infinite number positions; the argument is as follows. Assume $i < j$. In a block of length 2^j, where z^j is all 0s or all 1s, z^i has an equal number of 0s and 1s. Therefore, z^i and z^j differ in exactly half the positions in that block. Since there are an infinite number of blocks, they differ in infinite number of positions. So, each z^i belongs to a distinct class.

Permutations: for strings x, y, $x \approx y$ if one is a permutation of the other:
$abc \approx cba$.

Games Consider a 2×2 square in which there are 3 tiles named a, b, c. One of the squares is unoccupied; here shown by x. A tile can move horizontally or vertically to an unoccupied square. Can you reach every square from every other square?

$$\begin{array}{cccccccccccc} ab & ab & xb & bx & bc & bc & ax & xa & ca & ca & cx & xc \\ cx & xc & ac & ac & ax & xa & cb & cb & xb & bx & ba & ba \end{array}$$

Show that the transitive closure of the relation is an equivalence relation.

The story of the 15-puzzle.

Rubik's cube.

A baby is shown on the German TV to solve the puzzle in no time. Exploit symmetry.

Exercise: Is the intersection of two equivalence relations an equivalence relation? What about their union and product? Is the complement of an equivalence relation an equivalence relation?

The product of two equivalence relations is not an equivalence relation. Consider integers 1 through 5 as the domain of the relations. Let equivalence relations r and s be given by:

$$\begin{array}{lcl} x\ r\ y & \equiv & \lceil x/2 \rceil = \lceil y/2 \rceil \\ x\ s\ y & \equiv & \lfloor x/2 \rfloor = \lfloor y/2 \rfloor \end{array}$$

You can show $1\ (r \times\ s)\ 3$ and $3\ (r \times\ s)\ 5$. But $1\ (r \times\ s)\ 5$ does not hold.

2.4 Partial Order

Consider the prerequisite structure in CS. I show a small portion below.

The prerequisites need to be acyclic. A special kind of relation: reflexive, antisymmetric, transitive. Why does this gurantee acyclicity?

Example: $\leq$, divides, $\subseteq$ on 2^S. For $S = \{a, b, c\}$, see the relationship below; we have not drawn all the edges.

Set S is *partially-ordered* wrt $\leq$ if ...

Two items are comparable/incomparable.

Examples: Secure information flow. $x \leq y$ means x knows a subset of what y knows. That is, x tells everything it knows to y.

Choose between car models: criteria are price, performance, color.
$(a, b) \leq (c, d)$ means $a \leq c \wedge\ b \leq d$.

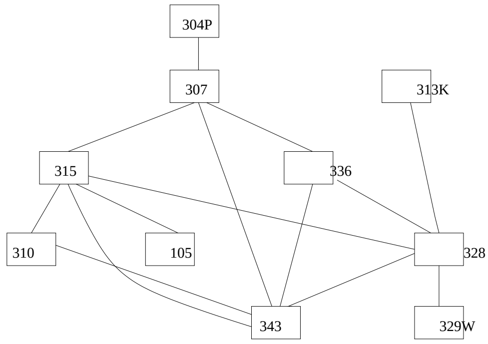

Figure 6: A Partial order

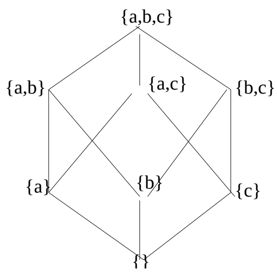

Figure 7: A Partial order

In real life, it is very difficult to find two entries where one dominates the other. To choose, you have to order the various criteria. You may order price, performance, color in this order. Color: pink $<$ yellow $<$ green $<$ white.

Price	Performance	Color
23,000	8	Green
18,000	6	Yellow
18,000	7	pink

We are stuck with the pink car.

Exercise School children are taught about the primary and secondary colors using a Venn diagram. Can you present the same material using partial orders? The primary colors are: Red, Blue and Green. Mixture of Red and Blue produces Magenta, Red and Green yields Yellow, Green and Blue gives Cyan, and the combination of all 3 colors gives White.

Lexicographic Order Dictionary order. A set of n-tuples can be ordered as follows:

$(a, b) < (c, d) \equiv a < c \ \vee \ (a = c \wedge b < d)$.
$(a, b) \leq (c, d) \equiv (a, b) < (c, d) \ \vee \ (a, b) = (c, d)$. That is,
$(a, b) \leq (c, d) \equiv a < c \vee \ (a = c \wedge b \leq d)$.

Decimal notation: $213 < 221 < 300$. We compare two numbers of differing lengths by appending 0s to the left of the shorter number, and then comparing them lexicopraphically.

In the dictionary: Strings s, t are of different lengths. Truncate the longer string, t, to the length of the shorter one, s. Call the truncated string t'.

$$t' < s \Rightarrow t < s$$
$$s < t' \Rightarrow s < t$$
$$s = t' \Rightarrow s < t$$

choice $<$ choose $<$ chosen.

Show that all strings can be totally ordered.

Total order: a partial order in which all pairs of items are comparable. Then, we can put them in a line in order, because of transitivity. Lexicographic Order is total. So is $<$ over reals, but not $\subseteq$ over sets.

Exercise You have a table of individuals in which each birthdate is recorded in mm/dd/yy format. How will you create a table in the sequence of birthdates, i.e., from the youngest to the oldest?

Partial Order over infinite sets: $\subseteq$ over subsets of naturals.

Exercise: Call an element x of a set minimal if no element is smaller. Call an element least if all elements are larger.

(1) Show that minimal and least are different concepts, (2) give examples of both, (3) show that every finite poset has a minimal element, though not necessarily a least element.

Exercise Topological sort.

Exercise; The partial order over partitions Consider the set of equivalence relations over a set D. Each equivalence relation induces a partition over D. We may order the partitions as follows: if a partition p can be obtained from another partition q by splitting some of its equivalence classes, then we say that p is *finer* than q, and q is *coarser* than p. Explore the properties of this relation. Is there a finest/coarsest partition? For any two partitions, is there a partition that is coarser (finer) than both?

3 Logic

Reading Assignment, Homework Read Rosen 1.1, 1.2, 1.3, 3.1
Homeworks:

1.2: 8, 14, 18, 20, 24, 41
1.3: 26, 32, 38, 44, 50
3.1: 4, 8, 10, 12, 20, 26, 40, 46, 47

3.1 Introduction

Why do we need logic? From physics with pictures to calculus.

From commonsense reasoning to logic.

Need akin to use of algebra.

Find all numbers whose squares are equal to the number itself.

Informal reasoning: Since the square is non-negative the number is itself non-negative. Clearly, 0 is a solution. From 0 to 1, the square is no greater than the number itself (multiplying by x, $0 < x < 1$ reduces any positive number). Thus no solution in the open interval $[0, 1]$. Another solution is 1. Beyond that multiplication by x increases a number; hence no more solutions.

Algebraic approach: Let the unknown be x. Solve $x^2 = x$. that is, $x^2 - x = 0$, or $x(x - 1) = 0$. This has the solutions $x = 0$ and $x - 1 = 0$.

3.2 A Proof Style

Proof Format The proof format shown below, due to W. H. J. Feijen, is a convenient tool for writing detailed proofs. Let $\Rightarrow$ denote any transitive relation (not necessarily implication over predicates) over proof terms. A proof term may be a predicate, arithmetic expression (in which case an arithmetic relation like $<$ or $\leq$ is used in place of $\Rightarrow$) or a property in Seuss logic. A proof of $p \Rightarrow s$ may be structured as follows.

$$\begin{array}{ll} & p \\ \Rightarrow & \{\text{why } p \Rightarrow q\} \\ & q \\ \Rightarrow & \{\text{why } q \Rightarrow r\} \\ & r \\ \Rightarrow & \{\text{why } r \Rightarrow s\} \\ & s \end{array}$$

3.2.1 A Property of Equivalence Relations

Let R_1, R_2 be two equivalence relations on some set. Define a relation R by

$$x\ R\ y \ \equiv\ (x\ R_1\ y)\ \wedge\ (x\ R_2\ y)$$

where x, y are elements of that set. Show that R is an equivalence relation.

R is reflexive:

$$\begin{array}{ll} & x\ R\ x \\ \equiv & \{\text{definition of } R\} \\ & x\ R_1\ x\ \wedge\ x\ R_2\ x \\ \equiv & \{R_1\text{, being an equivalence relation, is reflexive. Similarly, } R_2\} \\ & \textit{true}\ \wedge\ \textit{true} \\ \equiv & \{\text{logic}\} \\ & \textit{true} \end{array}$$

R is symmetric:

$$
\begin{array}{ll}
 & x \; R \; y \\
\equiv & \{\text{definition of } R\} \\
 & x \; R_1 \; y \;\wedge\; x \; R_2 \; y \\
\equiv & \{R_1\text{, being an equivalence relation, is symmetric. Similarly, } R_2\} \\
 & y \; R_1 \; x \;\wedge\; y \; R_2 \; x \\
\equiv & \{\text{definition of } R\} \\
 & y \; R \; x
\end{array}
$$

R is transitive:

$$
\begin{array}{ll}
 & x \; R \; y \;\wedge\; y \; R \; z \\
\equiv & \{\text{definition of } R\} \\
 & (x \; R_1 \; y \;\wedge\; x \; R_2 \; y) \;\wedge\; (y \; R_1 \; z \;\wedge\; y \; R_2 \; z) \\
\equiv & \{\text{rearranging the conjuncts}\} \\
 & (x \; R_1 \; y \;\wedge\; y \; R_1 \; z) \;\wedge\; (x \; R_2 \; y \;\wedge\; y \; R_2 \; z) \\
\Rightarrow & \{R_1\text{, being an equivalence relation, is transitive. Similarly, } R_2\} \\
 & x \; R_1 \; z \;\wedge\; x \; R_2 \; z \\
\equiv & \{\text{definition of } R\} \\
 & x \; R \; z
\end{array}
$$

3.2.2 Lowest Common Ancestor

This example combines several notions: commutativity, associativity of binary operators, partial order and proofs. In a given tree let $x \uparrow y$ denote the lowest common ancestor of nodes x, y. We show that $\uparrow$ is associative.

This result also applies to a partial order where $\uparrow$ is the least upper bound. The least upper bound may not always exist; when it exists it is unique.

Let $z \geq x$ denote that z is an ancestor of x. We assume the following properties.

1. Property 1: $\geq$ is a partial order.
2. Property 2: $z \geq x \uparrow y \equiv z \geq x \wedge z \geq y$.

Proposition 1 $[(x \uparrow y) \geq x] \wedge [(x \uparrow y) \geq y]$.

$$
\begin{array}{ll}
 & [(x \uparrow y) \geq x] \wedge [(x \uparrow y) \geq y] \\
= & \{\text{Let } z \text{ in property 2 be } x \uparrow y\} \\
 & (x \uparrow y) \geq (x \uparrow y) \\
= & \{\geq \text{ is reflexive}\} \\
 & true
\end{array}
$$

Proposition 2 $\uparrow$ is commutative.
Proof: We have to show $x \uparrow y = y \uparrow x$. We only show $x \uparrow y \geq y \uparrow x$; the other inequality is similarly proven.

$$
\begin{array}{ll}
& (x \uparrow y) \geq (y \uparrow x) \\
= & \{\text{Property 2}\} \\
& [(x \uparrow y) \geq y] \wedge [(x \uparrow y) \geq x] \\
= & \{\text{Proposition 1}\} \\
& \textit{true} \wedge \textit{true} \\
= & \{\text{Prdicate Calculus}\} \\
& \textit{true}
\end{array}
$$

Associativity of $\uparrow$ We show $(x \uparrow y) \uparrow z \geq x \uparrow (y \uparrow z)$. The reverse inequality is similarly proven.

$$
\begin{array}{ll}
& (x \uparrow y) \uparrow z \geq x \uparrow (y \uparrow z) \\
= & \{\text{Property 2}\} \\
& [(x \uparrow y) \uparrow z \geq x] \wedge [(x \uparrow y) \uparrow z \geq (y \uparrow z)] \\
= & \{\text{Proposition 1 applied twice: } (x \uparrow y) \uparrow z \geq (x \uparrow y) \geq x\} \\
& \textit{true} \wedge [(x \uparrow y) \uparrow z \geq (y \uparrow z)] \\
= & \{\text{property of } \wedge \text{ and Property 2}\} \\
& [(x \uparrow y) \uparrow z \geq y] \wedge [(x \uparrow y) \uparrow z \geq z] \\
= & \{\text{Proposition 1 applied twice: } (x \uparrow y) \uparrow z \geq (x \uparrow y) \geq y\} \\
& \textit{true} \wedge [(x \uparrow y) \uparrow z \geq z] \\
= & \{\text{Similarly}\} \\
& \textit{true}
\end{array}
$$

Exercise: Show that

1. $(x \uparrow x) = x$
2. $[(x \geq a) \wedge (y \geq b)] \Rightarrow [(x \uparrow y) \geq (a \uparrow b)]$

3.3 Propositional Logic

3.3.1 Laws

We consider the following propositional operators: $\wedge$ (and), $\vee$ (or), $\neg$ (not), $\equiv$ (equivalence), and $\Rightarrow$ (implication). The equality operator (=) is defined over all domains. Traditionally, it is written as $\equiv$ when applied to booleans; operator $\equiv$ has the lowest binding power among all logical operators whereas operator = has higher binding power than all logical operators except negation ($\neg$).

- (Commutativity and Associativity) $\wedge,\ \vee,\ \equiv$ are commutative and associative.
- (Idempotence) $\wedge, \vee$ are idempotent:
  $p \vee p \ \equiv\ p$
  $p \wedge p \ \equiv\ p$
- (Distributivity) $\wedge$, $\vee$ distribute over each other:
  $p \wedge (q \vee r) \ \equiv\ (p \wedge q) \vee (p \wedge r)$
  $p \vee (q \wedge r) \ \equiv\ (p \vee q) \wedge (p \vee r)$

- (Absorption)
$p \wedge (p \vee q) \;\equiv\; p$
$p \vee (p \wedge q) \;\equiv\; p$

- (Expansion)
$(p \wedge q) \;\vee\; (p \wedge \neg q) \;\equiv\; p$
$(p \vee q) \;\wedge\; (p \vee \neg q) \;\equiv\; p$

- (Laws with Constants)

$p \wedge$ *true*	$\equiv$	p	$p \wedge$ *false*	$\equiv$	*false*
$p \vee$ *true*	$\equiv$	*true*	$p \vee$ *false*	$\equiv$	p
$p \vee \neg p$	$\equiv$	*true*	$p \wedge \neg p$	$\equiv$	*false*
$p \equiv p$	$\equiv$	*true*	$p \equiv \neg p$	$\equiv$	*false*
true $\Rightarrow p$	$\equiv$	p	$p \Rightarrow$ *false*	$\equiv$	$\neg p$

- (Double Negation)
$\neg\neg p \;\equiv\; p$

- (De Morgan)
$\neg(p \wedge q) \;\equiv\; (\neg p \vee \neg q)$
$\neg(p \vee q) \;\equiv\; (\neg p \wedge \neg q)$

- (Implication operator)
$(p \Rightarrow q) \;\equiv\; (\neg p \vee q)$
$(p \Rightarrow q) \;\equiv\; (\neg q \Rightarrow \neg p)$
If $(p \Rightarrow q)$ and $(q \Rightarrow r)$ then $(p \Rightarrow r)$, i.e.,
$\langle (p \Rightarrow q) \wedge (q \Rightarrow r) \rangle \;\Rightarrow\; \langle p \Rightarrow r \rangle$

- (Equivalence)
$(p \equiv q) \;\equiv\; (p \wedge q) \vee (\neg p \wedge \neg q)$
$(p \equiv q) \;\equiv\; (p \Rightarrow q) \wedge (q \Rightarrow p)$

- (Monotonicity)
Let $p \Rightarrow r$. Then,
$(p \wedge q) \;\Rightarrow\; (r \wedge q)$
$(p \vee q) \;\Rightarrow\; (r \vee q)$

Strengthening, Weakening Predicate r *strengthens* (or, is a strengthening of) p if $r \Rightarrow p$; therefore, $p \wedge q$ strengthens p. Similarly, r *weakens* (or, is a weakening of) p if $p \Rightarrow r$; therefore, $p \vee q$ weakens p.

Priorities of Operators The logical operators in the decreasing order of priorities (binding powers) are: $\neg$, $=$, $\wedge$ and $\vee$, $\Rightarrow$, $\equiv$. Note that $=$ and $\equiv$ have different priorities though they have the same meaning when applied to boolean operands. Therefore, $p \wedge q = r \wedge s$ is equivalent to $p \wedge (q = r) \wedge s$ whereas $p \wedge q \equiv r \wedge s$ is $(p \wedge q) \;\equiv\; (r \wedge s)$. Operators $\wedge$ and $\vee$ have the same priorities, so we use parentheses whenever there is a possibility of ambiguity (as in $p \wedge q \vee r$). To aid the reader in parsing logical formulae visually, we often put extra whitespace around operators of lower priorities, as in $p \wedge q \;\equiv\; r \vee s$. We write $x, y = m, n$ as an abbreviation for $x = m \;\wedge\; y = n$.

3.3.2 Applications of Propositional Logic

- Show that $(p \equiv q) = (\neg p \equiv \neg q)$.

$$
\begin{array}{ll}
 & p \equiv q \\
= & \{\text{Double negation}\} \\
 & \neg\neg(p \equiv q) \\
= & \{\neg(p \equiv q) = (\neg p \equiv q)\} \\
 & \neg(\neg p \equiv q) \\
= & \{\text{commutativity of } \equiv\} \\
 & \neg(q \equiv \neg p) \\
= & \{\neg(r \equiv s) = (\neg r \equiv s)\} \\
 & \neg q \equiv \neg p \\
= & \{\text{commutativity of } \equiv\} \\
 & \neg p \equiv \neg q
\end{array}
$$

- For booleans a, b, x, y, z it is given that

$$x = a \ \wedge \ b \qquad y = \neg a \ \wedge \ \neg b \qquad z = [(x \ \vee \ y) \ \equiv b]$$

Express z as a function of a, b. Simplify your answer.

$$
\begin{array}{l}
\quad z \\
= \{\text{given}\} \\
\quad (x \ \vee \ y) \ \equiv \ b \\
= \{x = (a \ \wedge \ b), y = (\neg a \ \wedge \ \neg b)\} \\
\quad [(a \ \wedge \ b) \ \vee \ (\neg a \ \wedge \ \neg b)] \ \equiv \ b \\
= \{\text{simplify the term within square brackets}\} \\
\quad (a \ \equiv \ b) \ \equiv b \\
= \{\text{rearrange terms}\} \\
\quad a \ \equiv \ (b \ \equiv \ b) \\
= \{(b \ \equiv \ b) = \textit{true}\} \\
\quad a \equiv \textit{true} \\
= \{\text{property of } \equiv\} \\
\quad a
\end{array}
$$

- Show that $[p \equiv q] = [(p \Rightarrow q) \wedge (q \Rightarrow p)]$.

$$
\begin{array}{ll}
 & [(p \Rightarrow q) \wedge (q \Rightarrow p)] \\
= & \{\text{rewriting implication}\} \\
 & [(\neg p \vee q) \wedge (\neg q \vee p)] \\
= & \{\text{distributivity}\} \\
 & [(\neg p \wedge \neg q) \vee (\neg p \wedge p) \vee (q \wedge \neg q) \vee (q \wedge p)] \\
= & \{\text{Constants}\} \\
 & [(\neg p \wedge \neg q) \vee (\textit{false}) \vee (\textit{false}) \vee (q \wedge p)] \\
= & \{\text{Simplify and rearrange}\} \\
 & [(p \wedge q) \vee (\neg p \wedge \neg q)] \\
= & \{\text{Property of Equivalence}\} \\
 & p \equiv q
\end{array}
$$

Russell's Paradox: Let $S = \{x | x \notin x\}$. Thus $z \in S \equiv z \notin z$.

$$\begin{array}{ll} & S \in S \\ \equiv & \{\text{From above}\} \\ & S \notin S \end{array}$$

3.3.3 Playing with Exclusive Or

Exclusive or is the negation of $\equiv$, that is $(x \oplus y) = \neg(x \equiv y)$.

It is convenient to identify *false* with 0 and *true* with 1.

$x \oplus 0 = x$, $x \oplus 1 = \neg x$, $x \oplus x = 0$, $x \oplus \neg x = 1$.

$\oplus$ is commutative, associative, and it has an identity element (0) and an inverse (x is the inverse of x).

Example: Exchange registers a, b.

$a := a \oplus b;\ b := a \oplus b;\ a := a \oplus b.$

The following program, in which $\oplus$ is replaced by $\equiv$ also does the job.

$a := a \equiv b;\ b := a \equiv b;\ a := a \equiv b.$

Examples of the use of $\oplus$: Keeping a doubly linked list where each item has a single link field.

Encryption, decryption.

The game of Nim

Consider a cycle of 2^n numbers $x_0, ...$ In each step replace every x_i by $x_i \oplus x_{i+1}$, where $+$ in the subscript is modulo 2^n. Let X_i be the initial value of x_i. Show that after 2^k steps $x_i = X_i \oplus X_{i+2^k}$. Thus, eventually all numbers are zero.

Teaser Problem A cycle has 2^n integers $x_0..x_{2^n-1}$. In each step simultaneously for all i,

$x_i := |x_i - x_{i+1}|$, where arithmetic in the subscripts is modulo 2^n. Show that all x eventually become 0.

Exercise Given predicates r and s, show that the weakest solution to p in the following formulae is $(r \wedge b)\ \vee\ (s \wedge \neg b)$.

$$\begin{array}{l} p \wedge b \ \Rightarrow\ r \\ p \wedge \neg b \ \Rightarrow\ s \end{array}$$

That is $(r \wedge b)\ \vee\ (s \wedge \neg b)$ satisfies the two formulae given above, and if q is any solution then $q \Rightarrow \langle (r \wedge b)\ \vee\ (s \wedge \neg b) \rangle$. Note that the strongest solution for p is *false*.

Solution: We first show that $(r \wedge b) \vee (s \wedge \neg b)$ is a solution. Substituting $(r \wedge b) \vee (s \wedge \neg b)$ for p in the antecedent of the first formula:

$$\begin{array}{ll} & ((r \wedge b)\ \vee\ (s \wedge \neg b))\ \wedge\ b \\ \equiv & (r \wedge b \wedge b)\ \vee\ (s \wedge \neg b \wedge b) \\ \equiv & r \wedge b \\ \Rightarrow & r \end{array}$$

Substituting $(r \wedge b)\ \vee\ (s \wedge \neg b)$ for p in the antecedent of the second formula:

$$\begin{array}{ll} & ((r \wedge b)\ \vee\ (s \wedge \neg b))\ \wedge\ \neg b \\ \equiv & (r \wedge b \wedge \neg b)\ \vee\ (s \wedge \neg b \wedge \neg b) \\ \equiv & s \wedge \neg b \\ \Rightarrow & s \end{array}$$

Next, we show that $(r \wedge b)\ \vee\ (s \wedge \neg b)$ is as weak as any solution. That is for any solution q, $q\ \Rightarrow\ \langle (r \wedge b)\ \vee\ (s \wedge \neg b)\rangle$. So, we have to show

$$\langle ((q \wedge b)\ \Rightarrow\ r)\ \wedge\ ((q \wedge \neg b)\ \Rightarrow\ s)\rangle\ \Rightarrow\ \langle q\ \Rightarrow\ ((r \wedge b)\ \vee\ (s \wedge \neg b))\rangle$$

The proof is as follows.

$$\begin{array}{ll} & \langle (q \wedge b)\ \Rightarrow\ r\rangle\ \wedge\ \langle (q \wedge \neg b)\ \Rightarrow\ s\rangle \\ \Rightarrow & \{\langle (a \wedge c) \Rightarrow d\rangle\ \Rightarrow\ \langle (a \wedge c) \Rightarrow (d \wedge c)\rangle\} \\ & \langle (q \wedge b)\ \Rightarrow\ (r \wedge b)\rangle\ \wedge\ \langle (q \wedge \neg b)\ \Rightarrow\ (s \wedge \neg b)\rangle \\ \Rightarrow & \{\text{disjunction: } \langle (q \wedge b)\ \vee\ (q \wedge \neg b)\rangle\ \equiv\ q\} \\ & q\ \Rightarrow\ \langle (r \wedge b)\ \vee\ (s \wedge \neg b)\rangle \end{array}$$

Exercise Let $\oplus$ and $\otimes$ be binary boolean operators. We say that $\oplus$ is a *dual* of $\otimes$ if the following holds for all x and y.

$$\neg(x \oplus y)\ \equiv\ (\neg x \otimes \neg y)$$

1. Show that $\wedge$ is a dual of $\vee$.
2. Show that every binary boolean operator has a unique dual.
3. Show that $\otimes$ is a dual of $\oplus$ iff $\oplus$ is a dual of $\otimes$.
4. What is the dual of $\equiv$?
5. What is the dual of $\Rightarrow$?

Solution

1. Use De Morgan's law.
2. The dual $\oplus$ of $\otimes$ is uniquely defined by

   $$(x \oplus y)\ \equiv\ \neg(\neg x \otimes \neg y)$$

3. We have to show that

   $$(x \otimes y)\ \equiv\ \neg(\neg x \oplus \neg y)$$

The proof is as follows.

$$
\begin{array}{ll}
 & \neg(\neg x \oplus \neg y) \\
\equiv & \{\text{definition of } \oplus\} \\
 & \neg\neg(\neg\neg x \otimes \neg\neg y) \\
\equiv & \{\text{double negation}\} \\
 & x \otimes y
\end{array}
$$

4. Writing $\sim$ for the dual of $\equiv$, we have

$$
\begin{array}{ll}
 & x \sim y \\
\equiv & \{\text{definition of dual}\} \\
 & \neg(\neg x \equiv \neg y) \\
\equiv & \{(\neg x \equiv \neg y) \ \equiv \ (x \equiv y)\} \\
 & \neg(x \equiv y)
\end{array}
$$

Thus, $\sim$ is exclusive or.

5. Writing $\approx$ for the dual of $\Rightarrow$, we have

$$
\begin{array}{ll}
 & x \approx y \\
\equiv & \{\text{definition of dual}\} \\
 & \neg(\neg x \Rightarrow \neg y) \\
\equiv & \{(\neg x \equiv \neg y) \ \equiv \ (y \Rightarrow x)\} \\
 & \neg(y \Rightarrow x) \\
\equiv & \{\text{expanding } (y \Rightarrow x)\} \\
 & \neg(\neg y \vee x) \\
\equiv & \{\text{De Morgan}\} \\
 & y \wedge \neg x \\
\equiv & \{\text{Rearranging terms}\} \\
 & \neg x \wedge y
\end{array}
$$

3.4 Quantification

Notation For every number there is a larger number. This is typically written as
$\forall x.\exists y.y > x$, or $\forall x \exists y.y > x$.

We write:
($\forall x$ :: there is a number y larger than x), or
($\forall x$ :: ($\exists y$ :: y is larger than x)), or
$(\forall x :: (\exists y :: y > x))$.

To write this formula for natural numbers only:
($\forall x$: x natural : ($\exists y$: y natural : $y > x$)).

Every even number at least 4 is a sum of two primes:
($\forall x$: x even $\wedge$ $x \geq 4$: there exist two primes that add upto x), or
($\forall x$: x even $\wedge$ $x \geq 4$: ($\exists y, z$: y prime $\wedge$ z prime : $x = y + z$)).

We use quantification in writing arithmetic and boolean expressions. In all cases, a quantified expression is of the following form: $\langle \otimes x : \ q(x) : \ e(x) \rangle$. Here, $\otimes$ is any commutative, associative binary operator, x is the *bound* variable (or a list of bound variables), $q(x)$ is a predicate that determines the *range* of the bound variables and $e(x)$ is an expression called the *body*. A quantified expression in which the range is implicit is written in the following form: $\langle \otimes x \; :: \; e(x) \rangle$. We use other brackets in addition to angular brackets "$\langle$" and "$\rangle$" to delimit the quantified expressions. Some examples of quantified expressions are given below.

$$\langle + \, i : \; 0 \leq i \leq N : \; A[i] \rangle \tag{1}$$
$$\langle \forall i : \; 0 \leq i < N : \; A[i] \leq A[i+1] \rangle \tag{2}$$
$$\langle \forall i, j : \; 0 \leq i \leq N \; \wedge \; 0 \leq j \leq N \; \wedge \; i \neq j : \; M[i,j] = 0 \rangle \tag{3}$$
$$\langle min \, i : \; 0 \leq i \leq N \; \wedge \; (\forall j : \; 0 \leq j \leq N : \; M[i,j] = 0) : \; i \rangle \tag{4}$$
$$\langle max \, p : \; p \in P : \; p.next(t) \rangle \tag{5}$$

To evaluate a quantified expression: (1) compute all possible values of the bound variable x that satisfy range predicate $q(x)$, (2) instantiate the body $e(x)$ with each value computed in (1), and (3) combine the instantiated expressions in (2) using operator $\otimes$. In case the range is empty, the value of the expression is the unit element of operator $\otimes$; unit elements of some common operators are as given next, in parentheses following the operator: $+ \, (0), \; \times \, (1), \; \wedge \, ($*true*$), \; \vee \, ($*false*$), \; \equiv \; ($*true*$), \; min \, (+\infty), \; max \, (-\infty)$.

The values of the example expressions are as follows. Expression (1) is the sum of the array elements $A[0], \ldots, A[N]$. Expression (2) is *true* iff $A[0], \ldots, A[N]$ are in ascending order. Expression (3) has two bound variables; this boolean expression is *true* iff all off-diagonal elements of matrix $M[0..N, 0..N]$ are zero. Expression (4) is the smallest-numbered row in M all of whose elements are zero; if there is no such row the expression evaluates to ∞. Expression (5) is the maximum of all $p.next(t)$ where p is in P.

Examples Assume that x, y, z are integers in the following examples.
$(\forall x :: x^2 > x) =$ *false*.
$(\exists x :: x^2 > x) =$ *true*.
$(\forall x : 0 \leq x \leq 1 : (\exists y : y > 0 : y < x)) =$ *false*.

For every pair of distinct integers there is an integer that falls between them:
$(\forall x, y : x \neq y : (\exists z :: x < z < y \; \vee \; y < z < x))$, or
$(\forall x, y : x < y : (\exists z :: x < z < y))$.
This evaluates to *false*.

Matrix $A[0..M, 0..N]$ has a row of zeroes:
$(\exists i : 0 \leq i \leq M :$ row i is all zeroes), i.e.,
$(\exists i : 0 \leq i \leq M : (\forall j : 0 \leq j \leq N : A[j] = 0))$

The index of the lowest row in matrix $A[0..M, 0..N]$ that has ascending elements. Assume there is such a row.
$(\min i : 0 \leq i \leq M :$ row i is ascending), i.e.,
$(\min i : 0 \leq i \leq M : (\forall j : 0 \leq j \leq N : A[i,j] \leq A[i,j+1]))$

The number of non-zero elements in matrix A:
$(+i, j : 0 \le i \le M \ \wedge\ 0 \le j \le N \ \wedge\ A[i,j] \ne 0 : 1)$.

Free and Bound Variables The bound variables in a formula are explicitly declared, as explained earlier. The remaining variables are *free*. We adopt the convention that a formula is *universally quantified* over its free variables. Thus, read

$z \ge x \uparrow y \equiv z \ge x \wedge z \ge y$ to mean
$(\forall x, y, z ::\ z \ge x \uparrow y \equiv z \ge x \wedge z \ge y)$

3.4.1 Laws of Predicate calculus

In quantified boolean expressions, we often use the existential quantifier $\exists$ and universal quantifier $\forall$ in place of $\vee$ and $\wedge$. The following are some of the useful identities.

- (Empty Range)

$$\begin{array}{lcl} \langle \forall i :\ \mathit{false} :\ b \rangle & \equiv & \mathit{true} \\ \langle \exists i :\ \mathit{false} :\ b \rangle & \equiv & \mathit{false} \end{array}$$

- (Trading)

$$\begin{array}{lcl} \langle \forall i :\ q :\ b \rangle & \equiv & \langle \forall i ::\ q \Rightarrow b \rangle \\ \langle \exists i :\ q :\ b \rangle & \equiv & \langle \exists i ::\ q \wedge b \rangle \end{array}$$

- (Move-out) Given that i does not occur as a free variable in p,

$$\begin{array}{lcl} p \vee \langle \forall i :\ q :\ b \rangle & \equiv & \langle \forall i :\ q :\ p \vee b \rangle \\ p \wedge \langle \exists i :\ q :\ b \rangle & \equiv & \langle \exists i :\ q :\ p \wedge b \rangle \end{array}$$

- (De Morgan)

$$\begin{array}{lcl} \neg \langle \exists i :\ q :\ b \rangle & \equiv & \langle \forall i :\ q :\ \neg b \rangle \\ \neg \langle \forall i :\ q :\ b \rangle & \equiv & \langle \exists i :\ q :\ \neg b \rangle \end{array}$$

- (Range weakening) Given that $q \Rightarrow q'$,

$$\begin{array}{rcl} \langle \forall i :\ q' :\ b \rangle & \Rightarrow & \langle \forall i :\ q :\ b \rangle \\ \langle \exists i :\ q :\ b \rangle & \Rightarrow & \langle \exists i :\ q' :\ b \rangle \end{array}$$

- (Body weakening) Given that $b \Rightarrow b'$,

$$\begin{array}{lcl} \langle \forall i :\ q :\ b \rangle & \Rightarrow & \langle \forall i :\ q :\ b' \rangle \\ \langle \exists i :\ q :\ b \rangle & \Rightarrow & \langle \exists i :\ q :\ b' \rangle \end{array}$$

A number of identities can be derived from the trading rule (consult Gries and Schneider [1, Chapter 9]); we show two below.

$$\begin{array}{lcl}\langle \forall i :\ q \wedge r :\ b\rangle & \equiv & \langle \forall i :\ q :\ r \Rightarrow b\rangle \\ \langle \exists i :\ q \wedge r :\ b\rangle & \equiv & \langle \exists i :\ q :\ r \wedge b\rangle\end{array}$$

The following duals of the move-out rule are valid iff range q is not *false*.

$$\begin{array}{lcl}p \wedge \langle \forall i :\ q :\ b\rangle & \equiv & \langle \forall i :\ q :\ p \wedge b\rangle \\ p \vee \langle \exists i :\ q :\ b\rangle & \equiv & \langle \exists i :\ q :\ p \vee b\rangle\end{array}$$

3.4.2 Laws with Arithmetic Relations

The usual arithmetic relations are: $< = > \leq \neq \geq$. The first three are the only ones needed; the others can be defined in terms of them as follows.

$$\begin{array}{l}(x \leq y) \equiv (x = y \vee x < y) \\ (x \neq y) \equiv \neg(x = y) \\ (x \geq y) \equiv (x = y \vee x > y)\end{array}$$

The important properties of arithmetic relations are:

1. For any two reals (or integers or rationals) x, y, we have $(x < y) \vee (x = y) \vee (x > y)$.
2. $\leq$ and $\geq$ are total orders.
3. $=$ is an equivalence relation.
4. $\neq$ is symmetric, but neither reflexive nor transitive.
5. $x < y$ = $\neg(x \geq y)$.
   $x > y$ = $\neg(x \leq y)$.

3.4.3 Exercises with Predicate Calculus

1. Show that
   $(\forall i : q \wedge r : B)$ is same as $(\forall i : q : r \Rightarrow b)$, and
   $(\exists i : q \wedge r : b)$ is same as $(\exists i : q : r \wedge b)$.
2. Are the following pairs equal?
   $(\forall x : (\exists y :: P(x,y)))$ and $(\exists y : (\forall x :: P(x,y)))$.
   $(\exists x : (\exists y :: P(x,y)))$ and $(\exists y : (\exists x :: P(x,y)))$.
   $(\forall x : (\forall y :: P(x,y)))$ and $(\forall y : (\forall x :: P(x,y)))$.
3. Prove that all of the following are equal, using De Morgan
   $\neg(\exists x :: (\forall y :: P(x,y)))$,
   $(\forall x :: \neg(\forall y :: P(x,y)))$
   $(\forall x :: (\exists y :: \neg P(x,y)))$.
   Suppose $P(x,y)$ is x loves y. What do these sentences say?

4. Why are the following not valid even when p does not name i?

   $p \wedge (\forall i : q : b) \equiv (\forall i : q : p \wedge b)$
   $p \vee (\exists i : q : b) \equiv (\exists i : q : p \vee b)$

   Answer: For empty range:
   $p \wedge (\forall i : q : b)$ is p and $(\forall i : q : p \wedge b)$ is *true*. Therefore, if p is *false* these two are different.

   Also, for empty range:
   $p \vee (\exists i : q : b)$ is p and $(\exists i : q : p \vee b)$ is *false*. Therefore, if p is *true* these two are different.

5. Write the following statements formally.

   (a) Every integer is bigger than some integer and smaller than some integer.

   (b) There is no integer that is bigger than all integers.

   (c) For all nonzero integers there is a different integer having the same absolute value. (Use $|x|$ for the absolute value of x.)

   (d) No integer is both bigger and smaller than any integer.

   Solutions:

   (a) $(\forall\, x :\ x$ int:
   $\quad (\exists\, y :\ y$ int: $x > y)$
   $\quad \wedge\, (\exists\, z :\ z$ int: $x < z)$
   $)$

   (b) $\neg(\exists\, x :\ x$ int:
   $\quad (\forall\, y :\ y$ int: $x > y)$
   $)$

   (c) $(\forall\, x :\ x$ int $\wedge\, x \neq 0$:
   $\quad (\exists\, y :\ y$ int $\wedge\, x \neq y :\ |x| = |y|)$
   $)$

   (d) $\neg(\exists\, x : x$ int:
   $\quad (\exists\, y : y$ int: $x > y\ \wedge\ x < y)$
   $)$

6. Express the following. Given is a set S and a binary relation $*$ on it.

   (a) $*$ is reflexive,

   (b) $*$ is symmetric,

   (c) $*$ is transitive

   Solution:

   (a) $(\forall x :\ x \in S : x * x)$

9	2	6
7	4	0
5	3	1

Table 1: A Matrix with a saddle point

(b) $(\forall x, y:\ x \in S,\ y \in S : x * y \Rightarrow y * x)$

(c) $(\forall x, y, z:\ x \in S,\ y \in S,\ z \in S : (x * y\ \wedge\ y * z) \Rightarrow x * z)$

7. An item x of a subset is a *smallest* element if for every element y in that subset $x * y$. Element x of a subset is *minimal* in that subset if there is no y in that subset such that $y * x$. Express

   (a) the smallest element of S is unique,

   (b) a smallest element of S is a minimal element of S,

   (c) every subset of S, except the empty set, has a minimal element.

   Solution: In the following,
   $x\ smallest\ in\ T$ stands for $(\forall y:\ y \in T : x * y)$
   $x\ minimal\ in\ T$ stands for $\neg(\exists y:\ y \in T : y * x)$

   (a) $(\forall u, v:\ u \in S,\ v \in S :$
   $u\ smallest\ in\ S \wedge v\ smallest\ in\ S \Rightarrow u = v)$

   (b) $(\forall u:\ u \in S : u\ smallest\ in\ S \Rightarrow u\ minimal\ in\ S)$

   (c) $(\forall T:\ T \subseteq S \wedge T \neq \phi : (\exists u : u \in\ T : u\ minimal\ in\ T))$

3.4.4 An application: Saddle Point

Given is a matrix A of numbers. Henceforth, i, u range over the row indices and j, v over the column indices. An entry of the matrix is called a *saddle point* if it is the largest in its row *and* the smallest in its column. We will derive an algorithm to determine if the matrix has a saddle point. In the following example the bottom left entry is a saddle point. Are there any others?

Let
$hi[u] =$ the largest entry in row u, i.e, $hi[u] = (\max j :: A[u, j])$
$lo[v] =$ the smallest entry in column v, i.e, $lo[v] = (\min i :: A[i, v])$

Observation 1: From the definition of hi, lo, for all u, v,
$lo[v] \leq A[u, v] \leq hi[u]$.

Definition $A[u, v]$ is a saddle point iff $(A[u, v] = hi[u] \wedge A[u, v] = lo[v])$.

Observation 2 $A[u, v]$ is a saddle point $\equiv (hi[u] \leq lo[v])$.

$$\begin{array}{ccc|c} 9 & 2 & 6 & 9 \\ 7 & 4 & 0 & 7 \\ 5 & 3 & 1 & 5 \\ \hline 5 & 2 & 0 & \end{array}$$

Table 2: hi, lo values for the matrix in Table 1

$$\begin{array}{ll} & hi[u] \leq lo[v] \\ = & \{\text{Observation 1}\} \\ & (hi[u] \leq lo[v]) \wedge (lo[v] \leq A[u,v] \leq hi[u]) \\ = & \{\text{Predicate Calculus}\} \\ & A[u,v] = hi[u] \wedge A[u,v] = lo[v] \\ = & \{\text{Definition of saddle point}\} \\ & A[u,v] \text{ is a saddle point} \end{array}$$

The matrix has a saddle point if $(\exists u, v :: A[u,v]$ is a saddle point). Calculation shows:

$$\begin{array}{ll} & (\exists u, v :: A[u,v] \text{ is a saddle point}) \\ = & \{\text{Observation 2}\} \\ & (\exists u, v :: hi[u] \leq lo[v]) \\ = & \{\text{Arithmetic}\} \\ & (\min u :: hi[u]) \leq (\max v :: lo[v]) \end{array}$$

We now have an algorithm to detect if a matrix has a saddle point: compute the largest element of each row and the smallest of each column; check if the smallest among the former is less than or equal to the largest among the latter. In Table 2, we have computed the hi, lo values for the matrix in Table 1.

Using Observation 1 – $lo[v] \leq hi[u]$, for all u, v – we conclude that $(\min u :: hi[u]) = (\max v :: lo[v])$ if there is a saddle point, and this is also the value of the saddle point. Hence, the value of a saddle point is unique in a matrix, if one exists.

3.4.5 Associativity of Lowest Common Ancestor in a Tree

We redo the example of the lowest common ancestor of section 3.2.2. Using quantification shortens the proof by at least half. For instance, to prove that $\uparrow$ is commutative we no longer have to construct two proofs: $(x \uparrow y) \geq (y \uparrow x)$ and $(y \uparrow x) \geq (x \uparrow y)$.

Consider a partial order $\leq$ in which $x \uparrow y$, the least upper bound of x and y, is uniquely defined for all x and y. We derive certain properties of $\uparrow$, that it is commutative, associative, idempotent and monotonic. The partially-ordered set need not be finite.

The least upper bound may be defined as follows.

Definition: $x \uparrow y \leq z \;\equiv\; x \leq z \wedge y \leq z.$

It is easy to show that this definition matches the more conventional one:

$(x \le x \uparrow y) \ \wedge \ y \le x \uparrow y$, and
$(x \le t \ \wedge \ y \le t) \ \Rightarrow \ (x \uparrow y \le t)$

We give a few examples of $\uparrow$. Let $x \le y$ mean that y is an ancestor of x (assume x is its own ancestor) in a tree. Then $x \uparrow y$ is the least common ancestor of x and y according to this definition. As another example, let $x \le y$ mean that x divides y where x and y are positive integers. Then $x \uparrow y$ is the least common multiple of x and y. Also, $x \uparrow y$ denotes the maximum of x and y, where x and y are reals, and $x \le y$ has its standard meaning.

All the results given in this note also apply to the operator $\downarrow$ defined as follows:

$$z \le x \downarrow y \ \equiv \ z \le x \wedge z \le y.$$

For example, $x \downarrow y$ may denote the $\gcd$ of x and y for positive integers x and y. It may also denote $\min$ over numbers where $x \le y$ has its standard meaning.

Proposition 1: Indirect Proof of Ordering

$$(y \le x) \ \equiv \ (\forall w :: x \le w \ \Rightarrow \ y \le w)$$

Proof: For

$$(y \le x) \ \Rightarrow \ (\forall w :: x \le w \ \Rightarrow \ y \le w)$$

the proof is immediate. In the other direction, given $(\forall w :: x \le w \ \Rightarrow \ y \le w)$, set w to x to get $y \le x$.

Proposition 2: Indirect Proof of Equality

$$(x = y) \ \equiv \ (\forall w :: x \le w \ \equiv \ y \le w)$$

Proof: Apply proposition 1 to show $x \le y$ and $y \le x$.

Proposition 3: $\uparrow$ is commutative.
Proof: For any x, y, w

$$\begin{array}{ll} & x \uparrow y \le w \\ \equiv & \{\text{Definition}\} \\ & x \le w \ \wedge \ y \le w \\ \equiv & \{\text{Commutativity of } \wedge\} \\ & y \le w \ \wedge \ x \le w \\ \equiv & \{\text{Definition}\} \\ & y \uparrow x \le w \end{array}$$

From proposition 2, $(x \uparrow y) = (y \uparrow x)$. $\square$

Proposition 4: $\uparrow$ is associative.
Proof: For any x, y, z, w,

$$
\begin{array}{ll}
 & (x \uparrow y) \uparrow z \le w \\
\equiv & \{\text{Definition applied twice}\} \\
 & (x \le w \wedge y \le w) \wedge z \le w \\
\equiv & \{\text{Associativity of } \wedge\} \\
 & x \le w \wedge (y \le w \wedge z \le w) \\
\equiv & \{\text{Definition applied twice}\} \\
 & x \uparrow (y \uparrow z) \le w
\end{array}
$$

From proposition 2, $(x \uparrow y) \uparrow z = x \uparrow (y \uparrow z)$. □

A few properties of $\uparrow$ are readily provable:

1. (Idempotence) $x \uparrow x = x$.
2. (Monotonicity) $a \le x \wedge b \le y \ \Rightarrow\ a \uparrow b \le x \uparrow y$.

Proof of (2): Assume $a \le x \wedge b \le y$.

$$
\begin{array}{ll}
 & x \uparrow y \le w \\
\equiv & \{\text{Definition}\} \\
 & x \le w \wedge y \le w \\
\Rightarrow & \{\text{Premise: } a \le x \wedge b \le y\text{, and transitivity of } \le\} \\
 & a \le w \wedge b \le w \\
\equiv & \{\text{Definition}\} \\
 & a \uparrow b \le w
\end{array}
$$

Using proposition 1, $a \uparrow b \le x \uparrow y$.

A Small Derivation As an application of these results we prove that

$$(x \uparrow y \ = \ y \uparrow z) \ \Rightarrow\ (x \uparrow y \ = \ x \uparrow y \uparrow z)$$

In particular, $(\gcd(x, y) = \gcd(y, z)) \ \Rightarrow\ (\gcd(x, y) = \gcd(x, y, z))$.
Proof:

$$
\begin{array}{ll}
 & x \uparrow y \\
= & \{\text{idempotence}\} \\
 & (x \uparrow y) \uparrow (x \uparrow y) \\
= & \{x \uparrow y \ = \ y \uparrow z\} \\
 & (x \uparrow y) \uparrow (y \uparrow z) \\
= & \{\text{Commutativity and associativity of } \uparrow\} \\
 & x \uparrow (y \uparrow y) \uparrow z \\
= & \{\text{idempotence: } (y \uparrow y) \ = \ y\} \\
 & x \uparrow y \uparrow z
\end{array}
$$

3.5 Proof Methods

Aristotle-style Proof contrasted with Mathematical proof.

Givens:

1. Axioms/ Postulates, Premises, Previously proven theorems

2. Inference rules

Required: prove certain conclusions/theorem/propositions.

Typical steps are:

1. Mathematical modeling: Convert the problem from an informal description to a formal one.

2. Manipulation: Using the rules of logic.

3. Interpretation: convert logical deductions to the informal domain.

The structure of a theorem is often $p \Rightarrow q$; p is the hypothesis and q is the conclusion. The given inference rules and axioms have to be employed in the proof.

When you are unable to prove look for a counterexample.

Three-halves conjecture: start with 7. Ask them to do 27.

$P \neq NP$.

Fermat's conjecture.

Goldbach Conjecture.

3.5.1 Proof by Contradiction

Show that $\sqrt{2}$ is irrational.

The proof style is: assume $\sqrt{2}$ is rational; then derive a contradiction. Let $\sqrt{2}$ be m/n where m, n are integers having no common factors.

$$
\begin{array}{ll}
 & \sqrt{2} = m/n \wedge m, n \text{ have no common factors} \\
\Rightarrow & \{\text{Squaring}\} \\
 & m^2/n^2 = 2 \wedge m, n \text{ have no common factors} \\
\Rightarrow & \{\text{Arithmetic}\} \\
 & m^2 = 2 \times n^2 \wedge m, n \text{ have no common factors} \\
\Rightarrow & \{\text{Since } m^2 = 2 \times n^2,\ m \text{ is even, say } m = 2 \times s\} \\
 & m = 2 \times s \wedge n^2 = 2 \times s^2 \wedge m, n \text{ have no common factors} \\
\Rightarrow & \{\text{Since } n^2 = 2 \times s^2,\ n \text{ is even}\} \\
 & m = 2 \times s \wedge n \text{ is even } \wedge m, n \text{ have no common factors} \\
\Rightarrow & \{\text{Since } m, n \text{ are both even, they have a common factor, 2}\} \\
 & \textit{false}
\end{array}
$$

Thus, asked to prove $p \Rightarrow q$, we prove $(p \wedge \neg q) \Rightarrow$ *false*. In this case we were asked to show *true* $\Rightarrow \sqrt{2}$ irrational, and we showed $\sqrt{2}$ rational $\Rightarrow$ *false*. Proof by contradiction relies on the fact that $(p \Rightarrow q) \equiv ((p \wedge \neg q) \Rightarrow \textit{false})$.

$$
\begin{array}{ll}
 & (p \wedge \neg q) \Rightarrow \textit{false} \\
= & \{u \Rightarrow v \text{ is same as } \neg u \vee v\} \\
 & \neg(p \wedge \neg q) \ \vee \ \textit{false} \\
= & \{\text{Simplify}\} \\
 & \neg(p \wedge \neg q) \\
= & \{\text{De Morgan}\} \\
 & \neg p \ \vee \ q \\
= & \{u \Rightarrow v \text{ is same as } \neg u \vee v\} \\
 & p \Rightarrow q
\end{array}
$$

Exercise: Show that to prove $p \Rightarrow q$, it is sufficient to prove $(p \wedge \neg q) \ \Rightarrow \ q$.

3.5.2 Existence Proofs

Constructive Proof: There exists a prime larger than 100. Display one.
Show that for every positive integer n, there are n consecutive positive integers which are all composites. For $n = 2$, we have $8, 9$; for $n = 3$, the sequence $8, 9, 10$ works and for $n = 5$ take $24, 25, 26, 27, 28$. In general let $x = (n + 1)! + 1$. Take the n consecutive integers $x + 1, ..., x + i, ..., x + n$. Show that $x + i$ is divisible by $i + 1$, $1 \leq i \leq n$.

Non-constructive proof: There are irrationals a, b such that a^b is rational. consider $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}}$.

1. Case 1: The base $\sqrt{2}^{\sqrt{2}}$ is rational. Then $a, b = \sqrt{2}, \sqrt{2}$.
2. Case 2: The base $\sqrt{2}^{\sqrt{2}}$ is irrational. $(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\sqrt{2} \times \sqrt{2}} = \sqrt{2}^{2} = 2$. Thus, $a, b = \sqrt{2}^{\sqrt{2}}, \sqrt{2}$.

References

[1] David Gries and Fred B. Schneider. *A Logical Approach to Discrete Math*. Texts and Monographs in Computer Science. Springer-Verlag, 1994.