

Contents

Preface and Acknowledgements	iii
Sets, Relations, and Languages	1
Sets	1
Relations and Functions	3
Special Types of Binary Relations	3
Finite and Infinite Sets	7
Three Fundamental Proof Techniques	8
Closures and Algorithms	11
Alphabets and Languages	13
Finite Representations of Languages	16
Finite Automata	21
Deterministic Finite Automata	21
Nondeterministic Finite Automata	26
Finite Automata and Regular Expressions	32
Languages That Are and Are Not Regular	40
State Minimization	47
Algorithms for Finite Automata	51
Context-free Languages	57
Context-free Grammars	57
Parse Trees	63
Pushdown Automata	65
Pushdown Automata and Context-free Grammars	68
Languages That Are and Are Not Context-free	72
Algorithms For Context-free Grammars	79
Determinism and Parsing	81
Turing Machines	90
The Definition of a Turing Machine	90
Computing With a Turing Machine	95
Extensions of Turing Machines	97
Random Access Turing Machines	102
Nondeterministic Turing Machines	107
Grammars	108
Numerical Functions	113
Undecidability	115
The Church-Turing Thesis	115
Universal Turing Machines	115
The Halting Problem	116

Unsolvable Problems About Turing Machines	117
Unsolvable Problems About Grammars	121
An Unsolvable Tiling Problem	123
Properties of Recursive Languages	125
Undecidability	131
The class P	131
Problems, Problems	132
Boolean Satisfiability	135
The Class NP	137
NP-completeness	140
Polynomial-time Reductions	140
Cook's Theorem	141
More NP-complete problems	144
Coping With NP-completeness	148

Problem 1.1.1

- (a) **true.** Every set is a subset of itself, including \emptyset .
- (b) **false.** \emptyset has no members, not even \emptyset .
- (c) **true.** \emptyset is certainly a member of $\{\emptyset\}$, the set whose one and only member is \emptyset .
- (d) **true.** \emptyset is a subset of any set.
- (e) **true.** $\{a, b, c, \{a, b\}\}$ is the set whose elements are a , b , c , and $\{a, b\}$; clearly $\{a, b\}$ is one of these elements.
- (f) **true.** The members of $\{a, b\}$ are a and b , each of which is a member of $\{a, b, \{a, b\}\}$.
- (g) **false.** The members of $\{a, b\}$ are a and b , but every element of the powerset $2^{\{a, b, \{a, b\}\}}$ is a set.
- (h) **true.** Because $\{a, b\} \in \{a, b, \{a, b\}\}$, it is also true that $\{\{a, b\}\} \subseteq \{a, b, \{a, b\}\}$. By definition of the powerset, $\{\{a, b\}\} \in 2^{\{a, b, \{a, b\}\}}$.
- (i) **false.** $\{a, b, \{a, b\}\} - \{a, b\} = \{\{a, b\}\}$, not $\{a, b\}$.

Problem 1.1.2

- (a) $\{3, 5\}$
- (b) $\{3, 5, 7\}$
- (c) $\{1, 2, 7, 9\}$.
- (d) $\{\{8\}, \{7, 8\}, \{8, 9\}, \{7, 8, 9\}\}$

(e) $\{\{\}\}$ (which is, of course, the same as $\{\emptyset\}$).

Problem 1.1.3

(a) First, we show the \supseteq direction. Suppose that $x \in A \cup (B \cap C)$. Then, by the definition of set intersection one of two cases applies: either $x \in A$ or $x \in B \cap C$.

Suppose the former. Then, because $x \in A$, we know by the definition of set union that $x \in A \cup B$ and that $x \in A \cup C$. Because x is in both $A \cup B$ and $A \cup C$, by the definition of intersection, we conclude that $x \in (A \cup B) \cap (A \cup C)$.

On the other hand, suppose the latter – that $x \in B \cap C$. In this case, by the definition of intersection, it is true that $x \in B$ and $x \in C$. Applying the definition of union twice gives us that $x \in A \cup B$ and $x \in A \cup C$. From this, by the definition of intersection, we have $x \in (A \cup B) \cap (A \cup C)$.

Now we show the \subseteq direction. Suppose that $x \in (A \cup B) \cap (A \cup C)$. Then, by the definition of intersection, $x \in A \cup B$ and $x \in A \cup C$.

Suppose that $x \in A$. Then, by the definition of union, $x \in A \cup (B \cap C)$.

On the other hand, suppose $x \notin A$. Since $x \in A \cup B$, it must be the case that $x \in B$. Similarly, because $x \in A \cup C$, it must be true that $x \in C$. Thus, by definition of intersection, $x \in B \cap C$. Then, by definition of union, $x \in A \cup (B \cap C)$.

(b) Suppose $x \in A \cap (B \cup C)$. Then by definition of intersection $x \in A$ and $x \in (B \cup C)$. By applying the definition of union to the latter, either $x \in B$ or $x \in C$.

Suppose $x \in B$. Then, because $x \in A$, by definition of intersection $x \in A \cap B$. By definition of union, then, $x \in (A \cap B) \cup (A \cap C)$.

On the other hand, suppose $x \in C$. Then because $x \in A$, by definition of intersection $x \in A \cap C$. By definition of union, then, $x \in (A \cap B) \cup (A \cap C)$.

Suppose $x \in (A \cap B) \cup (A \cap C)$. Then either $x \in A \cap B$ or $x \in A \cap C$. Without loss of generality, suppose $x \in A \cap B$. Then $x \in A$ and $x \in B$, by definition of \cap . Because $x \in B$, by definition of \cup , $x \in B \cup C$. Because both $x \in A$ and $x \in B \cap C$, by definition of \cap , $x \in A \cap (B \cup C)$.

(c) Suppose $x \in A \cap (A \cup B)$. Then, by definition of intersection, $x \in A$ and $x \in (A \cup B)$. Since all we need to prove is that $x \in A$, we are done.

Suppose $x \in A$. Then, by definition of union, $x \in A \cup B$. By definition of intersection, $x \in A \cap (A \cup B)$.

(d) Suppose $x \notin A$. Then, by definition of intersection, $x \notin A \cap B$. Since neither $x \in A$ nor $x \in A \cap B$, by definition of union, $x \notin A \cup (A \cap B)$.

Suppose $x \in A$. Then by definition of union, $x \in A \cup (A \cap B)$.

(e) Suppose $x \in A - (B \cap C)$. Then $x \in A$ but $x \notin (B \cap C)$. By definition of intersection, either $x \notin B$ or $x \notin C$. Suppose, without loss of generality, that $x \notin B$. Then, because $x \in A$ but $x \notin B$, write $x \in A - B$, by definition of set difference. By definition of union, then, $x \in (A - B) \cup (A - C)$.

Suppose $x \in (A - B) \cup (A - C)$. Then either $x \in A - B$ or $x \in A - C$. Suppose, without loss of generality, $x \in A - B$. Then $x \in A$ but $x \notin B$. Because $x \notin B$, by definition of intersection, $x \notin B \cap C$. Thus $x \in A - (B \cap C)$, by definition of set difference, because $x \in A$.

Problem 1.1.4

(a) $\{\{a, b, c, d\}\}$ has the fewest members. $\{\{a\}, \{b\}, \{c\}, \{d\}\}$ has the most.

(b) The following partitions have exactly two members:

$$\begin{array}{ll} \{\emptyset, \{a, b, c, d\}\} & \{\{a\}, \{b, c, d\}\} \\ \{\{b\}, \{a, c, d\}\} & \{\{c\}, \{a, b, d\}\} \\ \{\{d\}, \{a, b, c\}\} & \{\{a, b\}, \{c, d\}\} \\ \{\{a, c\}, \{b, d\}\} & \{\{a, d\}, \{b, c\}\} \end{array}$$

1.2

 RELATIONS AND FUNCTIONS
Problem 1.2.1

(a) $\{(1, 1, 1), (1, 1, 2), (1, 1, 3), (1, 2, 1), (1, 2, 2), (1, 2, 3)\}$

(b) \emptyset

(c) $\{(\emptyset, 1), (\{1\}, 1), (\{2\}, 1), (\{1, 2\}, 1), (\emptyset, 1), (\{1\}, 2), (\{2\}, 2), (\{1, 2\}, 2)\}$

Problem 1.2.2

$$\begin{aligned} R \circ R &= \{(a, a), (a, b), (a, c), (a, d), (b, a), (b, b), (b, c)\} \\ R^{-1} &= \{(b, a), (c, a), (d, c), (a, a), (a, b)\}. \end{aligned}$$

R is not a function. $R \circ R$ is not a function. R^{-1} is not a function. In each case, both (a, a) and (a, b) are elements of the relation, making R multivalued.

Problem 1.2.3

(a) The function whose values are given by g but whose domain is $f(A)$ (this function is called the *restriction* of g to $f(A)$) must be onto.

(b) f must be one-to-one and the restriction of g to $f(A)$ must be one-to-one.

(c) f must be one-to-one and g must be a bijection between $f(A)$ and C .

Problem 1.2.4

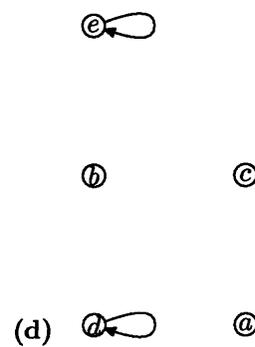
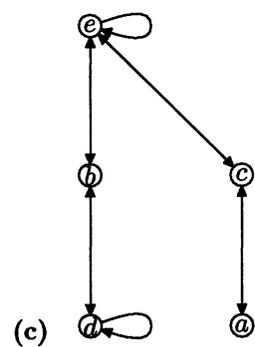
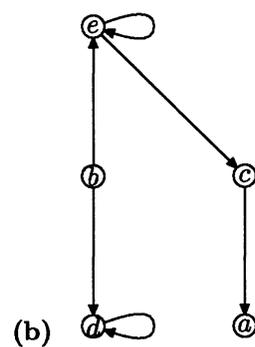
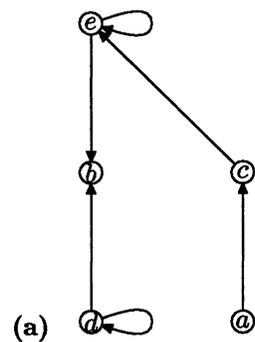
An element of $\{0, 1\}^A$ is a function $g : A \rightarrow \{0, 1\}$ – that is to say, a set of ordered pairs of the form (a, n) , where $a \in A$, n is 0 or 1, and there is exactly one pair (a, n) for each $a \in A$. Then $f : \{0, 1\}^A \rightarrow 2^A$, where $f(g)$ is the set $\{a : (a, 1) \in g\}$ will be the isomorphism we seek. Because $f(g) \subseteq A$, we have that $f(g) \in 2^A$, so f is a function.

Let us check that it is a bijection. If g and h are two different elements of $\{0, 1\}^A$, they are different functions $A \rightarrow \{0, 1\}$, so they must have different values for some $a \in A$. Without loss of generality, suppose $g(a) = 0$ and $h(a) = 1$. Then $a \notin f(g)$ (because $(a, 0) \in g$, it cannot also be the case that $(a, 1) \in g$, or else g would not be a function), whereas $a \in f(h)$. Thus $f(g) \neq f(h)$. Thus f does not take two distinct functions to the same set and is one-to-one.

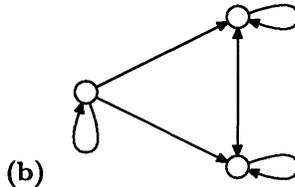
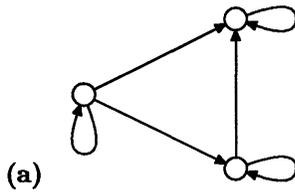
On the other hand, let $S \subseteq A$. Define the function $g(a) = \{1, \text{ if } a \in S; 0, \text{ otherwise}\}$. Then $f(g) = S$, so that f “hits” every subset of A and is thus onto 2^A .

1.3

 SPECIAL TYPES OF BINARY RELATIONS

Problem 1.3.1**Problem 1.3.2**

- (a) R is not reflexive, not symmetric, and not transitive. S is symmetric, but not reflexive or transitive.
- (b) $R \cup S$ is reflexive, but is neither symmetric nor transitive.

Problem 1.3.3**Problem 1.3.4**

(a) R is not reflexive. Take any random $a \in A$ – it is not the case that $(a, a) \in R$.

(b) R is symmetric. Since there are no a and b such that $(a, b) \in R$, we do not need to worry about ensuring that $(b, a) \in R$.

(c) R is anti-symmetric. Since there are no a and b such that $(a, b) \in R$, we do not need to worry about ensuring that $(b, a) \notin R$.

(d) R is transitive. Since there are no a, b , and c such that $(a, b) \in R$ and $(b, c) \in R$, we do not need to worry about ensuring that $(a, c) \in R$.

Problem 1.3.5

For any $a \in A$, it is true that $f(a) = f(a)$, so $(a, a) \in R$ for all $a \in A$. Thus R is reflexive.

Suppose $(a, b) \in R$. Then $f(a) = f(b)$, from which we know that $f(b) = f(a)$, so $(b, a) \in R$. Thus R is reflexive.

Suppose $(a, b) \in R$ and $(b, c) \in R$. Then $f(a) = f(b)$ and $f(b) = f(c)$, so that $f(a) = f(c)$, making $(a, c) \in R$. Thus R is transitive.

Problem 1.3.6

(a) R is a partial order. R is reflexive because every number is divisible by itself. R is anti-symmetric because if b is divisible by a (with $a \neq b$), then $a < b$, so it cannot be the case that a is divisible by b . R is transitive because if b is divisible by a then $b = na$, and similarly if c is divisible by b then $c = mb$. Then $c = nma$, so that c is divisible by a . R is not a total order – for many pairs of numbers a and b , it is not the case that neither a is divisible by b or that b is divisible by a (for example, $a = 2$ and $b = 3$).

(b) R is not a partial order, since it is not anti-symmetric. $((1, 2), (2, 1)) \in R$ and $((2, 1), (1, 2)) \in R$, but $(1, 2) \neq (2, 1)$. Since R is not a partial order, it is also not a total order.

(c) R is not a partial order, since it is not transitive. $(1, 2) \in R$ and $(2, 3) \in R$, but $(1, 3) \notin R$. Since R is not a partial order, it is also not a total order.

(d) R is not a partial order, since it is not anti-symmetric. “pizza”, at five letters, is no longer than “bagel”, also five letters. But “bagel” is also no longer than “pizza”. Since “pizza” \neq “bagel”, R is not anti-symmetric. Since R is not a partial order, it is also not a total order.

(e) R is a partial order. R is reflexive because every word is the same as itself. R is anti-symmetric because if a occurs more frequently than b , b cannot occur more frequently than a . R is transitive because if a appears more frequently than b and b more frequently than c , a must appear more frequently than c . R is not a total order because if two words a and b occur with equal frequency, then neither $(a, b) \in R$ nor $(b, a) \in R$. For example, “taxicab” and “ripoff” each occur exactly once in the text of the book (both on page 332).

Problem 1.3.7

$R_1 \cap R_2$ is reflexive. Let a be any element of A . Then, because both R_1 and R_2 are partial orders and thus reflexive, $(a, a) \in R_1$ and $(a, a) \in R_2$. Thus $(a, a) \in R_1 \cap R_2$.

$R_1 \cap R_2$ is anti-symmetric. Suppose $(a, b) \in R_1 \cap R_2$. Then $(a, b) \in R_1$ and $(a, b) \in R_2$. Because both R_1 and R_2 are partial orders and thus anti-symmetric, $(b, a) \notin R_1$ and $(b, a) \notin R_2$. Thus $(b, a) \notin R_1 \cap R_2$.

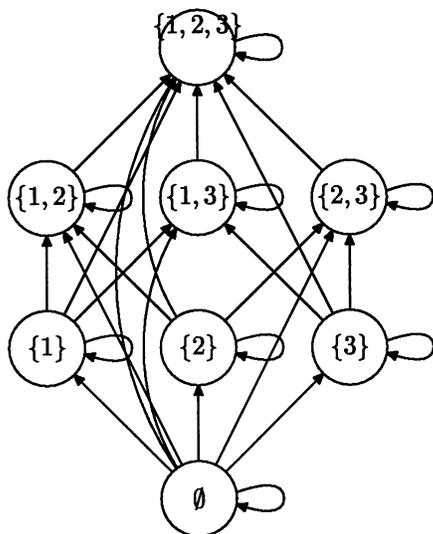
$R_1 \cap R_2$ is transitive. Suppose $(a, b) \in R_1 \cap R_2$ and $(b, c) \in R_1 \cap R_2$. Then $(a, b) \in R_1$, $(a, b) \in R_2$, $(b, c) \in R_1$, and $(b, c) \in R_2$. Because R_1 and R_2 are partial orders and thus transitive, $(a, c) \in R_1$ and $(a, c) \in R_2$. Therefore $(a, c) \in R_1 \cap R_2$.

Problem 1.3.8

(a) R_S is reflexive. Let A be any set in S . Because every set is a subset of itself, $A \subseteq A$, so that $(A, A) \in R_S$.

R_S is anti-symmetric. Suppose $(A, B) \in R$ and $A \neq B$. Then $A \subseteq B$. If $B \subseteq A$, this would mean that $A = B$ (by double inclusion), which we know is not the case. Thus $B \not\subseteq A$, so that $(B, A) \notin R$.

R_S is transitive. Suppose $(A, B) \in R$ and $(B, C) \in R$. Then $A \subseteq B$ and $B \subseteq C$. Because set inclusion is itself transitive, $A \subseteq C$. Thus $(A, C) \in R$.



(b) The minimal element under this order is \emptyset .

Problem 1.3.9

A directed graph represents a function when there is exactly one arrow (“edge”) leading out of each node.

Problem 1.3.10

Let a be any element of A . By repeated applications of f , we can form the sequence of elements $a, f(a), f(f(a)), f(f(f(a)))$. If there are n elements in A , the first $n + 1$ terms of this sequence must contain a duplicate (by the pigeonhole principle, introduced in section 1.5). Let a_i and a_j be a pair of duplicate elements with $i < j$ such that there is no other pair of duplicates a_k and a_l with $l - k < j - i$. Then the sequence $a_i, a_{i+1}, \dots, a_{j-1}, a_j$ is a cycle.

Problem 1.3.11

To show that R is a partial order, we need to show that it is reflexive, anti-symmetric, and transitive.

R is reflexive. Let Π be any partition of S . Because Π is a set of sets, for every $S \in \Pi$, it is the case that S is a set, and thus we can say that $S \subseteq S$. Since $S \in \Pi$, we have found the set containing S that we require. Since this works for any $S \in \Pi$, we conclude that $(\Pi, \Pi) \in R$.

R is anti-symmetric. Suppose $(\Pi_1, \Pi_2) \in R$, and that $\Pi_1 \neq \Pi_2$. Then there must be some set $X \in \Pi_1$ such that $X_1 \not\subseteq \Pi_2$. Because Π_1 refines Π_2 , there must be some set $X_2 \in \Pi_2$ such that $X_1 \subseteq X_2$. If $X_1 = X_2$, then we would have $X_1 \in \Pi_2$, so it must be the case that $X_2 \not\subseteq X_1$, meaning that there is some $x \in X_2$ but $x \notin X_1$. Further, because every set in a partition is non-empty, there must be some $y \in X_1$ – and because $X_1 \subseteq X_2$, we have that $y \in X_2$. But now, it cannot be the case that there is a set $Y \in \Pi_1$ such that $X_2 \subseteq Y$. X_1 cannot be such a Y , because it does not contain x . Any element of Π_1 other than X_1 , however, will fail to contain y – each element of S can belong to only one set in the partition, and y belongs to X_1 . Thus $(\Pi_2, \Pi_1) \notin R$, because we have found a counterexample to the condition that every set in Π_2 be included in some set in Π_1 .

R is transitive. Suppose $(\Pi_1, \Pi_2) \in R$ and $(\Pi_2, \Pi_3) \in R$. Let X_1 be any set in Π_1 . Because Π_1 refines Π_2 , there is some set $X_2 \in \Pi_2$ such that $X_1 \subseteq X_2$. Because Π_2 refines Π_3 , there is some set $X_3 \in \Pi_3$ such that $X_2 \subseteq X_3$. Thus $X_1 \subseteq X_3$, and for any set $X_1 \in \Pi_1$, we can find a set $X_3 \in \Pi_3$ with $X_1 \subseteq X_3$, so Π_1 refines Π_3 , and $(\Pi_1, \Pi_3) \in R$. There is a unique minimal element of this partial order – the partition $\{S\}$. There is also a unique maximal element of this partial order – the partition whose elements are those sets which each contain a single element of S .

If \mathcal{P} is not required to be made up of partitions, R need not be a partial order. For a counter-example, let $S = \{0, 1\}$. Let $\Pi_1 = \{\{0\}, \{0, 1\}\}$ and $\Pi_2 = \{\{1\}, \{0, 1\}\}$. It is true that $(\Pi_1, \Pi_2) \in R$, and also the case that $(\Pi_2, \Pi_1) \in R$, but $\Pi_1 \neq \Pi_2$, thus violating the anti-symmetry condition. R does, however, remain reflexive and transitive.

1.4	FINITE AND INFINITE SETS
-----	--------------------------

Problem 1.4.1

(a) If we do not require that our sets be disjoint, then the enumeration $\{a_0, b_0, c_0, a_1, b_1, c_1, \dots\}$ may suffer from the problem that some element or elements may appear more than once. For example, suppose that a_0 is the same as b_1 . We can easily avoid this problem, however, by “skipping” over duplicates the second or third time we encounter them. In this example, that would mean that our enumeration would start with $\{a_0, b_0, c_0, a_1, c_1, a_2, b_2, c_2, \dots\}$.

If any of the sets is finite, we can still represent it by an infinitely long sequence in which its elements repeat endlessly – that is, $\{1, 3, 5\}$ would become $\{1, 3, 5, 1, 3, 5, 1, 3, 5, \dots\}$. Once again, if we skip over duplicate elements each time we encounter them after the first, we have an enumeration in which each element is unique. If all three sets are finite, this enumeration will be a bijection between some finite subset of \mathbf{N} and their union; if at least one is infinite, it will be a bijection between \mathbf{N} and their union.

In general, to show that a set S is countable, we do not need to give a bijection $f : \mathbf{N} \rightarrow S$ – any onto function from the natural numbers to S will suffice, because it can be made into a bijection by the technique given above.

(b) Any finite set of natural numbers has a finite sum. For any fixed n , there are only finitely many ways of adding up distinct natural numbers to make n . For example, 3 can be written as $0 + 3$, or $0 + 1 + 2$, $1 + 2$, or just 3. For each $n \in \mathbf{N}$, let the set \mathbf{N}_n be the set of all sets of distinct natural numbers whose sum is n . Each \mathbf{N}_n is finite, and thus countable, and since there is exactly one set \mathbf{N}_n for each $n \in \mathbf{N}$, the set of all finite subsets of \mathbf{N} is the countably infinite union of the countable sets \mathbf{N}_n , and is therefore countable.

Problem 1.4.2

(a) Let f from \mathbb{N} to the odd natural numbers be given by $f(n) = 2n + 1$.

(b) Let f from the set of all integers to \mathbb{N} be given by

$$f(x) = \begin{cases} 2x - 1 & : x > 0 \\ -2x & : x \leq 0 \end{cases}$$

(c) Let $f : \mathbb{N} \times \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ be given by

$$f(i, j, k) = \frac{1}{6}(i + j + k)^3 + \frac{1}{2}(i + j)^2 + i$$

Problem 1.4.3

(a) By (1), $\emptyset \in C$. By (2), $\{\emptyset, \emptyset\} \in C$. We can rewrite $\{\emptyset, \emptyset\}$ as $\{\emptyset\}$. By (2), $\{\emptyset, \{\emptyset\}\} \in C$.

(b) Take the set S from part (a) and consider the set $S \times S$. This set can be written out as

$$\{(\emptyset, \emptyset), (\emptyset, \{\emptyset\}), (\{\emptyset\}, \emptyset), (\{\emptyset\}, \{\emptyset\})\}.$$

(c) No. Any set in C must be formed by one of the rules (1), (2), or (3). The empty set is finite, so rule (1) cannot make any infinite sets. Rule (2) makes sets which contain either 1 or 2 elements (depending upon whether $S_1 = S_2$), so rule (2) cannot make any infinite sets. Rule (3) make sets which contain $|S_1||S_2|$ elements, which is finite when both S_1 and S_2 are finite. Thus rule (3) cannot make infinite sets unless there already are infinite sets already in C . This argument is a simple example of *structural induction*, a technique of proof that will be useful repeatedly.

(d) C is countable. Let C_n be the set of elements of C which can be formed by at most n applications of rule (1), (2), or (3), and define C_0 to be \emptyset . In forming C_{n+1} from C_n , we have a choice of a finite number of rules to apply to a finite number of elements drawn from C_n . If C_n is finite, so then is C_{n+1} . By mathematical induction (see chapter 1.5), C_n is finite for all n . Every element of C must be the result of a finite number of applications of rules, and thus belongs to C_n for some $n \in \mathbb{N}$. Thus C is the countable union of the finite sets C_n , and is thus countable.

Problem 1.4.4

Consider the triangle with vertices $(0, 0)$, $(i + j - 1, 0)$, and $(0, i + j - 1)$. This triangle contains all the ordered pairs whose sum is less than $i + j$. The dovetailing method first visits all these pairs, then visits all pairs with sum $i + j$ but first value less than i , and then visits (i, j) .

The triangle contains $\frac{(i+j)(i+j+1)}{2}$ pairs, and there are i pairs with sum $i + j$ but smaller first value. Thus there are

$$m = \frac{(i + j)^2 + (i + j)}{(2)} + i = \frac{1}{2}[(i + j)^2 + 3i + j]$$

pairs enumerated before (i, j) . Since the enumeration starts with 0, this means that (i, j) is visited m th.

Problem 1.5.1

This result follows by induction on n .

Basis step. Suppose $n = 0$. Then:

$$0 \cdot 1 \cdot 2 = 0 = \frac{0(1)(2)(3)}{4}$$

Induction hypothesis. Given $n \geq 0$ assume that for all $k \leq n$:

$$1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + \cdots + k \cdot (k+1) \cdot (k+2) = \frac{k \cdot (k+1) \cdot (k+2) \cdot (k+3)}{4}$$

Induction step. Show true for $n+1$

$$\begin{aligned} 1 \cdot 2 \cdot 3 + \cdots + ((n+1) \cdot (n+2) \cdot (n+3)) &= 1 \cdot 2 \cdot 3 + \cdots + n \cdot (n+1) \cdot (n+2) + (n+1) \cdot (n+2) \cdot (n+3) \\ \text{(by inductive hypothesis)} &= \frac{n \cdot (n+1) \cdot (n+2) \cdot (n+3)}{4} + \frac{4 \cdot (n+1) \cdot (n+2) \cdot (n+3)}{4} \\ &= \frac{(n+1) \cdot (n+2) \cdot (n+3) \cdot (n+4)}{4} \end{aligned}$$

Problem 1.5.2

We show this result by induction on n .

Basis step. For $n = 0$, we have that $n^4 - 4n^2 = 0$, which is divisible by 3.

Induction hypothesis. Assume that $n^4 - 4n^2 = 3r$ for some $r \in \mathbb{N}$.

Induction step.

$$\begin{aligned} (n+1)^4 - 4(n+1)^2 &= n^4 + 4n^3 + 6n^2 + 4n + 1 - 4n^2 - 8n - 4 \\ &= n^4 + 4n^3 + 2n^2 + 4n - 3 \\ &= (n^4 - 4n^2) + 4n^3 + 6n^2 - 4n - 3 \end{aligned}$$

Applying the inductive hypothesis, we can substitute $3r$ for $n^4 - 4n^2$ to get

$$\begin{aligned} (n^4 - 4n^2) + 4n^3 + 6n^2 - 4n - 3 &= 3r + 2n(2n^2 + 3n - 2) - 3 \\ &= 3r + 2(n)(2n-1)(n+2) - 3 \end{aligned}$$

The first and third terms above are clearly divisible by 3; we need to show only that the middle term is also divisible by 3. n must be of the form $3s$, $3s+1$, or $3s+2$. If $n = 3s$, then n is divisible by 3. If $n = 3s+1$, then $n+2 = 3s+3$, which is divisible by 3. And if $n = 3s+2$, then $2n-1 = 6s+4-1 = 6s+3$, which is divisible by 3. In each case, the middle term is divisible by 3.

Problem 1.5.3

The problem is that the asserted base case of one horse is *not* the correct one. Consider the case when $n+1 = 2$. Call the horses in the set Bucephalus and Mister Ed. When you discard Bucephalus, “all the remaining horses,” meaning {Mister Ed}, “have the same color” by the inductive hypothesis. Call this color c_1 . Put Bucephalus back into the set and “discard another.” The only possibility is Mister Ed, so discard Mister. This time, “all the remaining horses,” referring to {Bucephalus}, “have the same color.” Call it c_2 . So Bucephalus and Mister Ed have the same color as “the ones that were not discarded either time,” which we shall call c_3 . That is, $c_1 = c_2 = c_3$. But when $n+1 = 2$, there are no horses in the set that were never discarded, so there are no horses of color c_3 to which we can apply the “is the same color as” relation to conclude $c_1 = c_3$ or $c_2 = c_3$, and no meaningful fixed value for c_3 . Since the induction fails to show that if the claim holds for 1 horses, then the claim holds for two horses, the entire proof fails.

Notice that if a proper base case were established, then the proof *does* show that all horses have the same color – if any set of two horses were all the same color, than any set of three would be, and so on.