Exercises supplementing those in Kenneth H. Rosen's *Discrete Mathematics and Its Applications*, 5th Edition

This is a collection of additional exercises that I put on homework sheets when teaching from the above text in Fall 2004 and Fall 2005, supplementing those in the book. Some I assigned, but most I described as for ''students interested in further interesting and/or more challenging problems'' to think about.

Some of these exercises have many parts. If I assigned them, I generally only asked the student to do the first few parts, the later ones being either more difficult, or too lengthy to include in homework that already had many other exercises.

(In a few cases, mainly toward the end of this packet, I give a problem which I think it would be interesting to work out, but which I haven't worked through myself. In these cases I indicate this clearly. If you are an instructor making use of this packet, you should, of course, first work out such an exercise if you plan to assign it. Apologies for including ''raw'' exercises of this sort; but they seemed interesting enough to justify it.)

I have given all these exercises numbers indicating the relevant section of the text, and continuing the numeration where the exercises in that section leave off, except, occasionally, when I have labeled one of my exercises as a variant of an exercise in the text, calling it N' where N was the number of the original exercise, or as an additional part of such an exercise. In all cases, the numbers I give my exercises are shown in quotation marks, to distinguish them from the exercises in the text.

George M. Bergman
gbergman@math.berkeley.edu
19 December, 2005

– = ≡ ≡ = –

§1.2, ''Exercise 62'': Show that $((p \to q) \wedge (r \to s)) \vee ((q \to r) \wedge (s \to p))$ is a tautology.

§1.3, ''Exercise 44′ and 45′'': In explaining existential and universal quantifiers, the author has not discussed the possibility that the universe of discourse might be empty; but this possibility must be taken into account.

For example, in studying mathematical problems such as Goldbach's Conjecture, i.e., the statement (which mathematicians have so far neither succeeded in proving nor disproving) that every even integer ≥ 4 can be expressed as the sum of two prime numbers, a mathematician might consider implications among various universal and existential statements whose universe of discourse was the set of even integers that could *not* be so expressed – not knowing whether that universe was empty or not.

With some thought, one can see that if $P(x)$ is any predicate whose universe of discourse has no members, then $\forall x\, P(x)$ is automatically true (there are no counterexamples!) while $\exists x\, P(x)$ is automatically false (there are no examples).

With this in mind, examine the four equivalences of §1.3 Exercises 44 and 45 (p.43), and determine which, if any, are valid in the sense that the two sides have the same truth value for *all* universes (empty or nonempty) and all predicates.

§1.3, ''Exercise 59'': Let the universe of discourse in this exercise be the set $\mathbf{Z}$ of all integers.

(a) For each of the three statement below, indicate which of the variables x and y is *free* and which is *bound*.

$$\exists x\ (2x = y), \qquad \exists y\ (2x = y), \qquad \forall y\ (2x = y).$$

(b) Regarding the first statement above as a predicate P in its free variable, the second statement as a predicate Q in its free variable, and the third as a predicate R in its free variable, say in words which integers n satisfy $P(n)$, which satisfy $Q(n)$, and which satisfy $R(n)$.

§1.4, ‘‘Exercise 54’’: Examine Rosen’s §1.4 Exercise 53 (p.56) and the answer to that exercise in the back of the book, to see what technique he uses to go from the words ‘‘infinitely many n’’ in the problem to a predicate expressed using arithmetic relations in his solution. Then

(a) Using the same technique, find a way of constructing, from any predicate $P(n)$ having the set $\mathbf{N}$ of natural numbers as its universe of discourse, a proposition which will be true if and only if $P(n)$ is true for infinitely many n.

(b) Can you likewise construct from a predicate $P(n)$ whose universe of discourse is the set $\mathbf{Z}$ of *all* integers a proposition that is true if and only if $P(n)$ holds for infinitely many n?

(c) Can you do the same for a predicate with the set $\mathbf{R}$ of all real numbers as its universe of discourse? (This can be done, but is more difficult. To do it without having taken a course like Math 104 (Real Analysis) requires a good intuitive understanding of the properties of the real numbers. If you do come up with a solution but are not sure it is correct, I applaud your healthy skepticism, and encourage you to ask me or your TA about it.)

§1.4, ‘‘Exercise 55’’: The notation $\exists!\, x\, P(x)$, ‘‘there exists a unique x such that $P(x)$ holds,’’ was introduced in §1.3, Exercise 48 (p.43) and also considered in Exercises 49 and 50 on that page. (In case you are not sure of the meaning of ‘‘unique’’, what that proposition says is that there exists a value of x for which $P(x)$ holds, but there do *not* exist more than one such value.)

If $Q(x,y)$ is a predicate in two variables, are the propositions

$$\exists!\, x\, \exists!\, y\, Q(x,y) \qquad \text{and} \qquad \exists!\, y\, \exists!\, x\, Q(x,y)$$

logically equivalent? Justify your answer with a proof (valid for all predicates Q on all universes of discourse) or a counterexample (i.e., a universe of discourse and a precise definition of Q on that universe for which the equivalence fails), as the case may be.

§1.5, ‘‘Exercise 78’’: Rosen’s §1.5 Exercise 77 (p.77) consists of an old argument for the non-existence of God, with the word ‘‘God’’ replaced by ‘‘Superman’’. As the answer in the back of the book indicates, the argument is valid, meaning that the conclusion follows from the hypotheses. Hence, someone who believes in God and who is logically consistent must consider at least one of the hypotheses, when applied to God, to be false.

If you believe in God, or feel you have a sympathetic understanding of the position of someone who does, say which of these hypotheses you or such a person would consider false. (In those hypotheses, understand ‘‘impotent’’ to mean ‘‘not omnipotent’’, and ‘‘to prevent evil’’ as meaning ‘‘to prevent all evil everywhere from occurring’’.)

Note: Deciding which hypotheses to reject may require thinking about nonmathematical questions, such as what it really means to *be able to* do something; and these questions can be quite difficult!

§1.7, ‘‘Exercise 54’’: For all sets A and B, prove that $(A \supseteq B) \leftrightarrow (\exists C\, (A = B \cup C))$.

§1.7, ‘‘Exercise 55’’: For all sets A and B, prove that $(A - B) \cup (A \cap B) = A$.

§1.7, ‘‘Exercise 56’’: Recall that in lecture I told you that if I is a nonempty set, and for each $i \in I$ we are given a set A_i, then mathematicians write

$$\bigcap_{i \in I} A_i \;=\; \{x \mid \forall\, i \in I,\; x \in A_i\}.$$

Now suppose such a set I and family of sets A_i are given; and for the purposes of this exercise, for each nonempty subset $J \subseteq I$ let us abbreviate $\bigcap_{i \in J} A_i$ to $A(J)$.

(a) If J is a subset of I, what inclusion relation must hold between $A(J)$ and $A(I)$?

In the remaining two parts, let J and J' be two subsets of I; we will consider the sets $A(J \cup J')$ and $A(J \cap J')$.

(b) Show that $A(J \cup J')$ can be expressed, using a set-operation, in terms of $A(J)$ and $A(J')$.

(c) Show that $A(J \cap J')$ *is not* determined by the sets $A(J)$ and $A(J')$. You can do this by finding, for some I, J and J', two different choices of the family of sets A_i $(i \in I)$ which might be called $A_i^{(1)}$ and $A_i^{(2)}$, such that applying the above definitions with the sets $A_i^{(1)}$ and $A_i^{(2)}$ in place of the sets A_i, one finds that $A^{(1)}(J) = A^{(2)}(J)$, and $A^{(1)}(J') = A^{(2)}(J')$, but $A^{(1)}(J \cap J') \neq A^{(2)}(J \cap J')$.

§1.7, ''Exercise 57'': If I is any set of more than one element, show that there exists a family of sets A_i $(i \in I)$ such that for every proper nonempty subset J of I, one has $\bigcap_{i \in J} A_i \neq \varnothing$, but such that $\bigcap_{i \in I} A_i = \varnothing$. (Here $\bigcap_{i \in I} A_i$ is defined as in the first sentence of the preceding exercise.)

§1.8, ''Exercise 72'': Suppose X and Y are sets, and $f: X \to Y$ is a function.

A function $g: Y \to X$ is called a *right inverse* to f if $fg = \iota_Y$, while a function $h: Y \to X$ is called a *left inverse* to f if $hf = \iota_X$. The function f is called *right invertible* if it has a right inverse, *left invertible* if it has a left inverse.

(a) Show that f is right invertible if and only if it is onto.

(b) Assuming X is nonempty, show that f is left invertible if and only if it is one-to-one.

(c) Show that f is both right invertible and left invertible if and only if it is invertible (bijective).

§1.8, ''Exercise 73'': (a) Of the four functions on the positive real numbers,

$$a_1(x) = x^2, \qquad a_2(x) = \lceil x^2 \rceil, \qquad a_3(x) = \lceil x \rceil^2, \qquad a_4(x) = \lceil \lceil x \rceil^2 \rceil,$$

show that two are equal, while the other two are distinct both from each other and from those two. (''Show'' always means ''prove''.)

(b) Of the four functions on the positive real numbers,

$$b_1(x) = x^{1/2}, \qquad b_2(x) = \lceil x^{1/2} \rceil, \qquad b_3(x) = \lceil x \rceil^{1/2}, \qquad b_4(x) = \lceil \lceil x \rceil^{1/2} \rceil,$$

show again that two are equal, while the other two are distinct both from each other and from those two.

§1.8, ''Exercise 74'': Let $f: X \to Y$ be a function. On p.110, in the preamble to Exercises 34-37, the author defines, for every subset $S \subseteq Y$, the subset $f^{-1}(S) \subseteq X$.

This is an important construction, but he should have emphasized that it is *not* a case of the concept of an inverse of a function, defined in Definition 9 (p.102), since here f is not assumed to be bijective – even though this operation and the inverse of a bijective function f are both written f^{-1}.

There are, however, close relationships between the two concepts, as we will see below.

(a) Recall that a *singleton* means a set with exactly one element. Show that f is a bijection if and only if for every singleton subset S of Y, the set $f^{-1}(S)$ (as defined on p.110) is a singleton subset of X.

(b) Find a similar condition on sets $f^{-1}(S)$ which you can show necessary and sufficient for f to be *injective*, and another which you can show necessary and sufficient for f to be *surjective*.

(c) Show that if f is bijective (so that the inverse map f^{-1} is defined), and S is any subset of Y, then the two sets that may be written $f^{-1}(S)$, namely the one defined on p.110 and the one gotten by taking the inverse function f^{-1} and applying it to the set S, are equal.

Note: *In the exercises for §2.2 below, I will, as discussed in class, write ''$f(x) \in O(g(x))$'' where Rosen says ''$f(x)$ is $O(g(x))$'', and similarly for the big-Ω and big-Θ relations.*

§2.2, ‘‘Exercise 64’’: Let two functions $a, b : \mathbf{Z}^+ \to \mathbf{Z}^+$ be defined by

$$a(n) = 2^{\lceil \log n \rceil}, \qquad b(n) = 2^{2^{\lceil \log(\log(n)) \rceil}}.$$

(a) Show that $a(n) \in \Theta(n)$.

(b) Show that $b(n) \in O(n^2)$ and $n \in O(b(n))$, but that $b(n)$ is neither in $\Theta(n)$ nor $\Theta(n^2)$.

§2.2, ‘‘Exercise 65’’: Find functions f and g from the positive real numbers to the positive real numbers such that $f \circ g$ is not $\Theta(g \circ f)$, and prove that it is not. (Suggestion: Experiment. For some sorts of choices of f and g you will see that $f \circ g$ must be $\Theta(g \circ f)$; so try functions of others sorts.)

§2.2, ‘‘Exercise 66’’: In this exercise, n will denote an integer-valued variable, while x will denote a real-valued variable.

Suppose f and g are functions from the positive real numbers to the positive real numbers, such that when we restrict the variable to integer values, we have $f(n) \in O(g(n))$.

(a) Under the above assumptions, show that if $f(x)$ and $g(x)$ are increasing functions, and if either $f(n+1) \in O(f(n))$ or $g(n+1) \in O(g(n))$, then $f(x) \in O(g(x))$. (Suggestion: First show that under either of these alternative conditions, one has $f(n+1) \in O(g(n))$.)

Thus, combining the above result with Example 6 on p.137, and observing that $n+1 \in O(n)$, we conclude that $\log(x) \in O(x)$ and that $x \in O(2^x)$ as functions of a *real* variable x.

(b) Investigate whether all the assumptions made in part (a) are needed. E.g., can you find counterexamples to the statement one gets if one drops the assumption that f is increasing? That g is increasing? That one of $f(n) \in O(f(n+1))$ or $g(n) \in O(g(n+1))$ holds?

§2.2, ‘‘Exercise 67’’: Let c be a positive real number.

(a) Show that $(\log x)^c \in O(x)$. In doing so you may assume the fact noted after ‘‘Exercise 66(a)’’ above, that $\log(x) \in O(x)$. (Suggestion: If you replace x with y^c in the desired relation, the resulting statement not hard to prove from that fact. Take the calculation involved and convert it into an argument in terms of x rather than y.)

(b) From part (a), prove that $x^c \in O(2^x)$.

§2.2, ‘‘Exercise 68’’: Find two increasing functions f, g from the positive real numbers to the positive real numbers such that neither $f(x) \in O(g(x))$ nor $g(x) \in O(f(x))$ is true.

(This is stronger than Exercise 41, since that exercise does not ask for increasing functions. Suggestion: Fiddle with the example in ‘‘Exercise 64(b)’’ above.)

§2.2, ‘‘Exercise 69’’: (a) Show: If m and n are natural numbers, then $x^m \in O(x^n)$ if and only if $m \leq n$.

(b) Prove for all natural numbers c that the function 2^x is not $O(x^c)$. You may assume the result of ‘‘Exercise 67(b)’’.

§2.2, ‘‘Exercise 70’’: You learned in beginning calculus (or precalculus) the concept of the limit of a function $f(x)$ as $x \to \infty$. Recall that as $x \to \infty$, a function f may approach a real number, or approach ∞, or not approach any limit.

Suppose f and g are functions from the positive real numbers to the positive real numbers.

(a) Show that if $\lim_{x \to \infty} f(x)/g(x)$ exists and is a nonzero real number, then $f(x) \in \Theta(g(x))$.

(b) Find an example where $f(x) \in \Theta(g(x))$ but $\lim_{x \to \infty} f(x)/g(x)$ does not exist.

(c) Show that if $\lim_{x \to \infty} f(x)/g(x) = 0$, equivalently, if $\lim_{x \to \infty} g(x)/f(x) = \infty$, then $f(x) \in O(g(x))$ but $g(x) \notin O(f(x))$.

(d) Find an example where $f(x) \in O(g(x))$ and $g(x) \notin O(f(x))$, but $\lim_{x\to\infty} f(x)/g(x)$ does not exist.

§2.2, ''Exercise 71'': (a) Suppose f, g and h are functions from positive real numbers to positive real numbers, such that $\lim_{x\to\infty} f(x) = \infty$. Show that if $g(x) \in O(h(x))$, then $(g\circ f)(x) \in O((h\circ f)(x))$.

(b) Does the result of part (a) remain true if we remove the assumption that $\lim_{x\to\infty} f(x) = \infty$?

(c) Under the assumptions of part (a), and the additional assumptions that $\lim_{x\to\infty} g(x) = \lim_{x\to\infty} h(x) = \infty$, can we conclude that $(f\circ g)(x) \in O((f\circ h)(x))$? (Hint: See §2.2, Exercise 36, p.143.)

§2.2, ''Exercise 72'': Rosen has marked §2.2 Exercises 51-59 with the words ''(calculus required),'' because they concern little-*o* notation, which he defines in the paragraph before Exercise 51 in terms of a limit. However, go back to the definition of limit that you learned in calculus, apply it to the limit he writes down, simplify the resulting statement, and thus show that his definition of $f(x)$ being $o(g(x))$ can be written in a form similar to, and almost as simple as, the definition of $f(x)$ being $O(g(x))$.

§2.3, ''Exercise 29'': (a) Given integers $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$, write down an algorithm that will check whether any a_i is equal to any b_j, namely, that will set the variables e and f equal to values such that $a_e = b_f$ if such exist, while if not, it will set $e = f = 0$.

(b) Determine a big-*O* estimate for the number of comparisons used by the algorithm of part (a), showing your reasoning.

(c) Suppose now that we are given *sorted* sequences of integers $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$, i.e., that $a_1 \leq \ldots \leq a_n$ and $b_1 \leq \ldots \leq b_n$. In this case, obtain an algorithm that gets the same result as in part (a), but using only $O(n)$ comparisons, and prove this bound on its complexity. (Hint: If for some h you have found a k such that $b_k < a_h < b_{k+1}$, note that a_h cannot equal any of the b_j's, and that in testing a_{h+1} for equality with the b_j's, you only need compare it with those after b_k.)

§2.4, ''Exercise 61'': Let m be an integer >1, and let u and v be rational numbers which can each be written with denominator relatively prime to m. Let us agree to write $u \equiv v \pmod{m}$ if the rational number $u-v$, when written with denominator relatively prime to m, has numerator divisible by m.

(a) To justify the above definition, show that for m, u and v as in the first sentence above, $u-v$ can indeed be written with denominator relatively prime to m, and that when it is so written, the question of whether its numerator is divisible by m does not depend on the choice of that denominator.

(b) Show that the condition $u \equiv v \pmod{m}$ is also equivalent to saying that whenever u and v are written with a *common* denominator relatively prime to m, then their numerators are congruent to one another mod m.

(c) Show that when $u, v \in \mathbf{Z}$, the above definition of $u \equiv v \pmod{m}$ is equivalent to the usual one (as given in the text).

(d) For u, v, w with denominators relatively prime to m, show that if $u \equiv v \pmod{m}$ and $v \equiv w \pmod{m}$ then $u \equiv w \pmod{m}$.

(e) Show that for every rational number u whose denominator is relatively prime to m, there exists one and only one $r \in \{0, 1, \ldots, m-1\}$ such that $u \equiv r \pmod{m}$ (where r is regarded as a rational number with denominator 1).

(f) Show that for this definition of congruence mod m, Theorem 10, p.163, remains true if the integers a, b, c, d are replaced by arbitrary rational numbers whose denominators are relatively prime to m.

§2.5, ''Exercise 56'': On p.180 just before Exercise 30, Rosen defines the n-bit ''one's complement representation'' of an integer x in the range $-2^{n-1}+1 \le x \le 2^{n-1}-1$, and on pp.180-181, just before Exercise 36 he defines the n-bit ''two's complement representation'' of an integer x in the range $-2^{n-1} \le x \le 2^{n-1}-1$.

(a) Show that the n-bit one's complement representation of an integer x in the former range is just the binary representation of the nonnegative integer $x\ \mathbf{mod}\ (2^n-1)$. Show also that there is exactly one string of n bits that is *not* the one's complement representation of any integer in this range. What is that string?

(b) Show that the n-bit two's complement representation of an integer x in the latter range is the binary representation of the nonnegative integer $x\ \mathbf{mod}\ 2^n$, and that every string of n bits is the two's complement representation of such an integer.

(c) Do Exercise 35 in the text using the result of part (a) above.

(d) Do Exercise 41 in the text using the result of part (b) above.

§2.5, ''Exercise 57'': The ancient Babylonians wrote their numbers in what is called ''sexagesimal'', i.e., ''base 60'' notation; but in fact, it was a mixture of base 10 and 6 notations. The positions in their numbers had values 1, 10, 60, 600, 3600, 36000, etc., the value of each position being alternately 10 times and 6 times that of the position before, so that the notation for a number n corresponded to an expression

$$n = a_0 + 10\,a_1 + 60\,a_2 + \ldots + 10^i 6^i a_{2i} + 10^{i+1} 6^i a_{2i+1} + \ldots,$$

where for j even, $0 \le a_j < 10$, while for j odd, $0 \le a_j < 6$. (I suppose this was based on the way number-words were formed in their language.)

(a) In the above expression for n, I used two formulas for the general summand, one for the case where the subscript on a is even, namely, $2i$, and one for the odd case, where it is $2i+1$. Using the ceiling and/or floor function(s), write a single formula that works for both cases. Show the final term, with coefficient a_k, which I omitted above.

(b) Write in pseudocode an algorithm to take a positive integer n and express it in the Babylonian system, i.e., to generate the digits $a_0, a_1, \ldots, a_k$ in the above expression for n.

§2.5, ''Exercise 58'': This exercise would be a great deal of work, and I haven't attempted it myself; but it is interesting to think about it, and if it appeals to you, you might like to work on it.

Let n be a nonnegative integer, and consider three nonnegative integers

$$a = (a_n \ldots a_1\, a_0)_2, \qquad b = (b_n \ldots b_1\, b_0)_2, \qquad c = (c_n \ldots c_1\, c_0)_2,$$

each written using $n+1$ digits in base 2. (Here we allow a_n, b_n, c_n to be zero, so that if we rewrite a, b and c so as to start with the first *nonzero* digit, they are integers of *at most* $n+1$ binary digits.)

For each $i \le n$, let p_i denote the proposition ''$a_i = 1$'', q_i the proposition ''$b_i = 1$'', and r_i the proposition ''$c_i = 1$''.

(a) Describe a way of generating from these $3n+3$ propositions, and the logical operators $\wedge$, $\vee$, $\rightarrow$, $\neg$, a *compound proposition* P which will hold if and only if the arithmetic statement $a \cdot b = c$ is true.

Of course, one could do this by listing all 2^{n+1} possibilities for a and all 2^{n+1} possibilities for b, and forming the disjunction of the $(2^{n+1})^2$ propositions specifying the digits of a and b

in every possible way, and giving the correct digits for their product c. But you should, instead, base your construction on the algorithm for multiplication to base 2.

(b) Obtain a big-O estimate for the length of the proposition P constructed as in part (a), as a function of n. Use the number of occurrences of the propositions $p_0, \ldots, r_n$ as your measure of ‘‘length’’. (So, for instance, the compound proposition $p_1 \vee (\neg p_0 \wedge \neg q_0)$ would be considered to have length 3.)

(c) Suppose you allow yourself to use not only the given propositions p_i, q_i and r_i, but also additional propositions with unspecified interpretations. Then it might be possible to construct a compound proposition Q in the given propositions and these new ones, such that $a \cdot b = c$ holds if and only if Q is *satisfiable,* meaning that there exist some truth values for the new propositions which, together with the specified values for the p_i, q_i and r_i, make Q true. If so, can you do this in such a way as to get a better (i.e., smaller) estimate for the length of Q than you were able to get for the length of P in part (a)?

(For example, there might be propositions s_{ijk} which are thought of as meaning that at a certain stage in the base-2 calculation of $a \cdot b = c$ determined by i, j and k, a ‘‘1’’ is carried. To use auxiliary propositions in this way, you would have to work into Q terms that guarantee that Q could only be satisfied if the truth-value of s_{ijk} is actually equal to that of the statement that a 1 is carried at that point.)

(d) Using the results of (a) and/or (c), show how the problem of factoring an integer of n binary digits can be transformed into one of finding truth-values, if any, that cause a compound proposition to be satisfied. (Cf. paragraph in Rosen beginning at bottom of p.149.)

§2.6, ‘‘Exercise 61’’: (a) Show that if p and q are distinct odd primes, then there are four solutions to $x^2 \equiv 1 \pmod{pq}$, no two of which are congruent to each other modulo pq, and such that every solution to that congruence is congruent modulo pq to exactly one of those solutions.

(The above wording is messy. The way mathematicians like to say this is that ‘‘up to congruence modulo pq, there are exactly four solutions to $x^2 \equiv 1 \pmod{pq}$’’.) Hint: Use Exercise 15 for each of p and q, and the Chinese Remainder Theorem.

(b) If $p_1, \ldots, p_n$ are n distinct odd primes, how many solutions, up to congruence modulo $p_1 \ldots p_n$, will the congruence $x^2 \equiv 1 \pmod{p_1 \ldots p_n}$ have? (No proof asked for.)

§2.7, ‘‘Exercise 38’’: Let α denote the function from the set of nonnegative real numbers to the set $\{0, 1\}$ such that $\alpha(0) = 0$, while for all positive x one has $\alpha(x) = 1$. (You can think of ‘‘α’’ as standing for ‘‘all or nothing’’.) If $\mathbf{A}$ is any matrix of nonnegative real numbers, let $\alpha(\mathbf{A})$ denote the zero-one matrix obtained from $\mathbf{A}$ by applying α to each of its entries.

(a) Suppose $\mathbf{A}$ and $\mathbf{B}$ are matrices with nonnegative real entries. Show that if the shapes of these matrices are such that $\mathbf{A}+\mathbf{B}$ is defined, then $\alpha(\mathbf{A}+\mathbf{B}) = \alpha(\mathbf{A}) \vee \alpha(\mathbf{B})$. Likewise, show that if the shapes of our given matrices are such that $\mathbf{AB}$ is defined, then $\alpha(\mathbf{AB}) = \alpha(\mathbf{A}) \odot \alpha(\mathbf{B})$.

(b) Assuming the associativity of ordinary matrix addition and multiplication, deduce using the results of part (a) the associativity of the operations $\vee$ and $\odot$ on zero-one matrices.

§3.1, ‘‘Exercise 52’’: Generalizing the idea of Exercise 47, suppose we have a jug full of water holding $a + b$ gallons, and empty jugs that can hold a gallons and b gallons respectively, where $a \leq b$ are relatively prime integers. Show that you can measure any integer number of gallons $\leq a + b$.

(Suggestion: Show that if you can measure c gallons, where $c < b$, then you can also measure $(c + a) \ \mathbf{mod}\ b$ gallons. What volumes will repetition of this process allow you to get? In thinking about the first part of this suggestion, you might draw a graph where the y-coordinate shows the amount of water in the jug that can hold a gallons and the x-coordinate the amount in the jug that holds b gallons, and figure out what the allowable operations look like graphically.)

§3.2, ''Exercise 46'': Show that if $f: X \to Y$ is a function, and the set X is countable, then $f(X)$ is also countable.

§3.3, ''Exercise 79'': *Strong induction with no base case.*

Suppose P is a propositional function on the natural numbers.

(a) Translate into words the proposition

$$(\forall\, n \in \mathbf{N}\, ((\forall\, m \in \mathbf{N}\, ((m < n) \to P(m))) \to P(n))) \to (\forall\, n \in \mathbf{N}\ P(n)).$$

(b) Let P be any propositional function on the natural numbers such that $P(0) = \mathbf{F}$. Verify that P satisfies the above proposition by determining the truth-values of the two sides of the last implication.

(c) Now prove, using the result of (b) and the principle of strong induction as stated in Rosen, that the proposition of (a) holds for every P.

(d) Prove the proposition shown in (a) directly from the well-ordering property of the natural numbers.

(e) Verify that the proposition stated in (a) remains true if $\mathbf{N}$ is replaced by any well-ordered set.

§3.4, ''Exercise 66'': (a) Given the values of two successive Fibonacci numbers, f_{n-1} and f_n, work out formulas expressing f_{n+1}, f_{n+2}, f_{n+3}, f_{n+4} and f_{n+5} in terms of these.

(b) From the results of part (a), conjecture a formula expressing f_{n+m} in terms of f_{n-1}, f_n, and some numbers that depend only on m.

(c) Prove by some form of induction the formula you conjectured in part (b).

(d) Using the formula from (c), develop formulas that express f_{2n-1} and f_{2n} in terms of f_{n-1} and f_n.

Remark: Combining (d) above with the idea of Algorithm 5 on p.176, one can calculate f_b using $O(\log b)$ arithmetic operations.

§3.4, ''Exercise 67'': In this exercise, a ''formal fraction'', will mean an expression ''m/n'' where m and n are relatively prime nonnegative integers. Thus, all formal fractions can be considered to represent nonnegative rational numbers, with the single exception ''$1/0$''. (Intuitively, $1/0$ represents ''∞'', but that is not a rational number.)

Consider the following recursive construction, which at the nth step gives a sequence F_n of 2^n+1 formal fractions: Let F_0 be the two-term sequence $(0/1, 1/0)$. Given F_k, the sequence F_{k+1} will consist of the terms of F_k, with one new term inserted between each pair of successive old terms; namely, if successive old terms were a/b and a'/b', we insert $(a+a')/(b+b')$ between them. We will call F_k the kth *Farey sequence*. (These are a variant of what are usually called Farey sequences. The relationship is explained at the end of the exercise.)

(a) Show that each F_k, if we drop the final term $1/0$, represents a strictly increasing sequence of nonnegative rational numbers.

We now wish to show that every nonnegative rational number appears in the sequence F_k for some k. We will first need some easier-to-prove facts:

(b) Show that in a sequence F_k, if the mth term from the beginning is a/b, then the mth term from the end is b/a.

(c) Show that for all $k \geq 0$, F_{k+1} has, as successive terms, the two formal fractions $k/1$ and $(k+1)/1$.

Notice that since $k/1$ and $(k+1)/1$ occur as successive terms in F_{k+1}, they will continue to occur as terms, though no longer successive, in all later Farey sequence F_{k+m}.

(d) Show for all $m \geq 1$ and $k \geq 0$ that if the terms between $0/1$ and $1/1$ in the sequence F_m are a_1/b_1, a_2/b_2, a_3/b_3, ..., then the terms between $k/1$ and $(k+1)/1$ in the sequence F_{k+m} are equal to $k+(a_1/b_1)$, $k+(a_2/b_2)$, $k+(a_3/b_3)$, ... (I say ''are equal to'' rather than ''are'' because I have not written these terms as formal fractions. The expressions in the latter form will be $(kb_1+a_1)/b_1$, $(kb_2+a_2)/b_2$, $(kb_3+a_3)/b_3$, ...)

I claim that these facts can be used to ''find'' any positive rational number in some Farey sequence. For instance, suppose we want to find where $2/7$ occurs. Well, if it occurs in some Farey sequence F_k, then by (b), the mirror-image position in that same sequence will have $7/2 = 3½$. Applying (d) with $k=3$, we see that the position where $3½$ occurs between 3 and 4 in a Farey sequence F_{3+m} corresponds to the position where $½$ occurs between 0 and 1 in the Farey sequence F_m.

This is easy to locate among the first few Farey sequences. But if we haven't computed these, we can still find the position by repeating the idea: $1/2$ must occur in the mirror-image position to $2/1$, and now (c) tells us where to find that.

The above discussion was stated in terms of ''finding'' a rational number in a Farey sequence, assuming it occurred. But you should be able to use the same ideas to

(e) Prove that (the expression in lowest terms for) every nonnegative rational number occurs in some Farey sequence F_k.

Incidentally, if you compare the above analysis of where a given rational number a/b will show up in a Farey sequence with the steps of the Euclidean algorithm applied to a and b, you will find a close connection.

Relation between the above definition and the standard definition of Farey sequence: In the standard definition, the first sequence is given as $(0/1, 1/1)$ instead of $(0/1, 1/0)$, so that we don't have the ''meaningless'' term $1/0$. However, that version only gives the rationals between 0 and 1. It is not hard to show that that standard version of the Farey sequence can be obtained from the one presented here either by taking, as the nth step, the first 2^n+1 terms of the $2^{n+1}+1$-term sequence I have called F_{n+1}, or by replacing each term a/b of F_n by $a/(a+b)$. Inversely, my version can be obtained from the standard one either by replacing each term a/b by $a/(b-a)$, or by combining each sequence with its ''mirror image'' in the sense of part (b) above.

§3.4, ''Exercise 68'': *Some observations on the* $3x+1$ *function.*

Our text states the $3x+1$ conjecture (pp.221-222) in terms of the function f such that if x is even, $f(x) = x/2$, while if x is odd, $f(x) = 3x+1$. Note that in the latter case, $f(x) = 3x+1$ will be even, so the next step will always be to divide by 2. Hence there is a well-known variant formulation of the problem in which these two steps are collapsed together, and we use instead of f the function g defined by

$$g(x) = x/2 \text{ if } x \text{ is even}$$
$$g(x) = (3x+1)/2 \text{ if } x \text{ is odd.}$$

Note that each of the cases of the above definition of g can give either an even or an odd value for $g(x)$; so after a step of either sort, the next step can also be of either sort.

Let us define the ''pattern'' associated with an integer x to be the sequence of letters e and o, where the first term is e if x is even and o if x is odd, the second term is e if $g(x)$ is even and o if $g(x)$ is odd, the third term is e if $g(g(x))$ is even, o if it is odd, and so forth. (For instance, you can check that the pattern associated with 7 begins *oooeoeeoeeeo...*.)

Since for positive x, $(3x+1)/2 > x$, we see that o's in the pattern correspond to steps at which the value increases, and e's to steps at which it decreases.

(a) Show that if $x \equiv y \pmod{2^n}$, then the first n terms of the patterns associated with x and y

are the same.

(b) Show that if $x \equiv y \pmod{2^n}$ but $x \not\equiv y \pmod{2^{n+1}}$, then the $n+1$st terms of the patterns associated with x and y are different.

(c) Does the result of (b) remain true if we delete the assumption that $x \equiv y \pmod{2^n}$?

(d) Deduce from (a) and (b) that for every finite sequence s of e's and o's, there exist positive integers whose associated patterns begin with s; and that if n is the length of s, then all integers whose patterns begin with s are congruent to one another mod 2^n.

(e) Deduce in particular that for every positive integer n, there exist positive integers x such that $x < g(x) < \ldots < g^n(x)$, where g^n here denotes the result of composing g with itself n times.

Remarks: Though the above shows that we can ''control'' the beginning of the behavior of an integer under repeated application of the function g, once the point up to which we have ''controlled'' it is past, we can expect, statistically, that e's and o's will occur in about equal numbers, unless the terms ''settle down'' to some periodic behavior. Now at each o the value is multiplied by approximately $3/2$, while at each e it is multiplied by $1/2$, so with n o's and n e's it will be multiplied by approximately $(3/2)^n(1/2)^n = (3/4)^n$, which approaches 0 as $n \to \infty$. So in general, we can expect that under repeated application of g, numbers will ''drift'' downwards from large values to smaller ones, though with many short-term increases during the downward drift.

Similar though more complicated arguments allow one to make a plausible estimate of the likelihood that x starts a periodic pattern, i.e., satisfies $g^m(x) = x$ for some m, so that when one starts with x – or starts with any other values and eventually hits x – the values will thereafter repeat every m terms. As calculations eliminate the possibility of such behavior for small $x \neq 1, 2$, we are left with lower and lower probabilities that it will happen for the remaining larger values of x. Calculations based on this idea indicate that it is highly likely that all positive integers eventually reach 1. But it does not seem likely that these probabilistic arguments can be turned into a proof. If there is one, it must bring in some different methods. We will look from a different standpoint at the question of periodic behavior in the next exercise.

Further note: If one modifies the functions f and g by replacing $3x+1$ by $3x-1$, it turns out that alongside the numbers that eventually give 1, there are numbers that eventually settle down to different periodic sequences of terms; you should be able to find at least one such sequence with very little experimentation! All the same probabilistic reasoning is applicable to that function as to the $3x+1$ function, *except* for the absence of observed periodic behavior for small values of x. But for that difference, those arguments would imply (incorrectly), that the $3x-1$ operation could be expected to eventually bring every positive integer to 1.

Incidentally, the study of the $3x-1$ function for positive x is easily seen to be equivalent to the study of the $3x+1$ function for negative x.

§3.4, ''Exercise 69'': Let the function g, and the ''pattern'' of e's and o's determined by an integer x, be defined as in the preceding exercise. In this exercise, we shall examine the possibility that an integer determines a periodic pattern. We first need

(a) Prove that if two integers x and y determine the same pattern, then they are equal. (Suggestion: Use part (d) of the preceding exercise.)

(b) Show that no positive integer x determines the pattern *oooooo...* with only o's. (Suggestion: If x determines this pattern, what will be the expression for $g(x)$ in terms of x, and what pattern will $g(x)$ determine? Solve the resulting equation for x.)

Let us write o^∞ for the pattern referred to above, and generally, if s is a finite string of o's and e's, let us write s^∞ for the infinite string obtained by endlessly repeating the string s. Now

(c) Investigate similarly the questions of whether there exist positive integers that determine the patterns e^∞, $(oe)^\infty$, $(ooe)^\infty$, $(oee)^\infty$, and $(ooee)^\infty$.

(d) Without computation, deduce from the results of part (c) the answers to the corresponding questions for the patterns $(eo)^\infty$, $(oeo)^\infty$, $(eoo)^\infty$, $(eoe)^\infty$, $(eeo)^\infty$, and three others.

Remark: If you solved the equations arising in part (c), you will have gotten solutions some of which were not integers. By the idea of ‘‘§2.4, Exercise 61’’, one can regard any rational number u with odd denominator as ‘‘$\equiv 0 \pmod 2$’’ or ‘‘$\equiv 1 \pmod 2$’’, i.e., ‘‘even’’ or ‘‘odd’’, according to whether its numerator is even or odd. Hence one can extend the function g to such rational numbers. The calculations referred to show that if we extend the $3x+1$ problem to these values, we do *not* always end up with ‘‘1’’. (In fact, we can never end with 1 unless the denominator of the number we start with is a power of 3. It is an open question whether every rational number with odd denominators eventually settles down to a periodic pattern.)

§3.4, ‘‘Exercise 70’’: Let S be the set of bit-strings defined recursively by the three conditions

(i) The length-1 string 0 belongs to S.

(ii) If s belongs to S then so does any bit-string obtained from s by replacing some occurrence of the bit 0 by the string 100 (i.e., if $x0y \in S$, then $x100y \in S$).

(iii) S contains no strings other than those so obtained.

To get a characterization of the set S, let us, for any bit-string s, write $l(s)$ for the length of s (the number of characters in s), and for any $m \leq l(s)$, let $n_0(s,m)$ denote the number of 0's among the first m bits of s, and $n_1(s,m)$ the number of 1's among those bits. (So $n_0(s,m) + n_1(s,m) = m$.)

(a) Prove that if $s \in S$, then $n_0(s, l(s)) = n_1(s, l(s)) + 1$, while for all positive integers $m < l(s)$, one has $n_0(s,m) \leq n_1(s,m)$.

(b) Prove, conversely, that if s is a bit-string such that $n_0(s) = n_1(s) + 1$, and such that for all positive $m < l(s)$ one has $n_0(s,m) \leq n_1(s,m)$, then $s \in S$. (Key step: If s satisfies these conditions and is not the string 0, show that the last 1 in s must be followed by at least two 0's.)

§3.4, ‘‘Exercise 71’’: In discussing recursively defined sets, Rosen speaks of a *basis step*, a *recursive step*, and an *exclusion rule* (p.261 bottom and p.262 top), the last being the statement that the recursively defined set contains *nothing but* the elements given in the basis step and the elements generated from these by repeated applications of the recursive step.

Mathematicians, rather than talking about an ‘‘exclusion rule’’, generally call this a ‘‘minimality condition’’. This exercise will show the properties that make that term appropriate. For simplicity and concreteness, we will not consider an arbitrary recursive construction, but will assume a construction given in which new elements are generated from old ones using just two operations: a function f that constructs a new element $f(x)$ from a single old element x, and another function, g, that constructs a new element $g(x,y)$ from each *pair* (x,y) of old elements.

(For instance, in the definition of a certain class of well-formed compound propositional formulas, f might be the function such that for each formula E, one has $f(E) = (\neg E)$, and g the function such that for formulas E and F, one has $g(E,F) = (E \rightarrow F)$.)

So let U be any set, the universe within which we will be performing our recursive construction, let $S_0 \subseteq U$ be a subset, our ‘‘basis set’’, and let $f: U \rightarrow U$ and $g: U \times U \rightarrow U$ be two functions.

To describe the subset S of U recursively constructed from S_0 using f and g, let us recursively define sets S_i $(i \geq 0)$:

S_0 is given.

For $i > 0$, assuming S_{i-1} has been defined, let

(1) $$S_i \;=\; S_{i-1} \,\cup\, f(S_{i-1}) \,\cup\, g(S_{i-1} \times S_{i-1}).$$

Once all these sets S_i are defined, let

(2) $$S \;=\; \bigcup_{i=0}^{\infty} S_i\,.$$

This expresses Rosen's presentation of a recursive construction: His ''exclusion principle'' is implicit in (2), since that puts no elements into S other than those that have been constructed in one of the steps (1).

The viewpoint that leads us to call this a *minimality condition* instead of an exclusion principle is the following. We describe S as a set which satisfies

(3) $$S_0 \subseteq S, \qquad f(S) \subseteq S, \qquad g(S \times S) \subseteq S,$$

and which is *minimal* for that property, meaning that for every set $T \subseteq U$ which similarly satisfies

(4) $$S_0 \subseteq T, \qquad f(T) \subseteq T, \qquad g(T \times T) \subseteq T,$$

we have

(5) $$S \subseteq T.$$

(a) Prove that these descriptions are equivalent; i.e., prove that if S is constructed from S_0 by (1) and (2), then it is a subset of U that satisfies both (3) and the statement

(6) $$\forall\, T \subseteq U\; ((4) \rightarrow (5)).$$

Prove also that no other subset $S' \neq S$ of U satisfies (3) and (6). The latter result says S is the *unique* set satisfying these conditions.

Mathematicians describe the properties (3) and (6) by calling S the *least* subset $T \subseteq U$ satisfying (4).

Is the construction via (1) and (2) the only way to prove that there *exists* a least set satisfying (4)? No. Here is another.

(b) Forgetting the definition of S by (1) and (2), let S denote the *intersection* of all subsets $T \subseteq U$ that satisfy (4). (The set of such sets T is nonempty, since U itself is such a set.) Show that this set S will satisfy (3) and (6).

Thus, by the uniqueness statement in (a), the set S constructed this way is the same as the one constructed via (1) and (2).

Let us now see how proofs by structural induction can be justified when recursive constructions are described in this way.

(c) Suppose P is a property of certain elements of U, such that

(7) $$\text{(i) } \forall\, x \in S_0\; (P(x)) \qquad\qquad \text{(ii) } \forall\, x \in U\; (P(x) \rightarrow P(f(x)))$$
$$\text{(iii) } \forall\, x, y \in U\; ((P(x) \wedge P(y)) \rightarrow P(g(x,y)))$$

Prove, for the set S constructed by (1) and (2), equivalently, characterized by (3) and (6), equivalently, constructed as in part (b) above, that

(8) $$\forall\, x \in S\; (P(x)).$$

Suggestion: Show that $T = \{x \in U \mid P(x)\}$ satisfies (4).

§3.4, ''Exercise 72'': For all nonnegative integers n, let us define compound propositions $P_n(p_1, \ldots, p_{2^n})$ in 2^n propositions $p_1, \ldots, p_{2^n}$ by the recursive conditions

$P_0(p_1)$ is p_1.

If P_{n-1} has been defined, then $P_n(p_1, \ldots, p_{2^n})$ is the proposition

$$P_{n-1}(p_1, \ldots, p_{2^{n-1}}) \longleftrightarrow P_{n-1}(p_{2^{n-1}+1}, \ldots, p_{2^n})$$

Find and prove a simple description of P_n, which expresses the truth-value of $P_n(p_1, \ldots, p_{2^n})$ for a given assignment of truth-values to $p_1, \ldots, p_{2^n}$ in terms of how many of those values are **T** and how many are **F**.

§3.4, ''Exercise 73'': Rosen notes on p.258, start of paragraph before Example 3, that recursively defined functions are ''well defined''. As I explained in class, this means that the conditions describing such a function have the property that there exists one and only one function satisfying them.

In this exercise we will see the nontriviality of this assertion, by noting a couple of descriptions of functions that resemble recursive descriptions, but that do not yield well defined functions.

Let $[0,1]$ denote $\{x \in \mathbf{R} \mid 0 \leq x \leq 1\}$.

(a) Suppose we attempt to define a function $f: [0,1] \to \mathbf{R}$ by the conditions that $f(0) = 0$, while for $a > 0$,

$$f(a) = 1 \text{ if for all } b \text{ with } 0 \leq b < a \text{ we have } f(b) = 0,$$
$$f(a) = 0 \text{ otherwise.}$$

Show that there exists *no* function f satisfying these conditions.

(b) Suppose we attempt to define a function $f: [0,1] \to \mathbf{R}$ by the conditions that $f(0) = 0$, while for $a > 0$,

$$f(a) = 0 \text{ if for all } b \text{ with } 0 \leq b < a \text{ we have } f(b) = 0,$$
$$f(a) = 1 \text{ otherwise.}$$

Show that there exist *more than one* function f satisfying these conditions. (In fact, there are infinitely many, but I only ask you to find at least two.)

(c) Show that the results of (a) and (b) remain true if $[0,1]$ is replaced by $\mathbf{Q} \cap [0,1]$ (i.e., the set of rational numbers between 0 and 1) or by $\{0\} \cup \{1/n \mid n \in \mathbf{Z}^+\}$. (But in the last of these cases, there are only two functions in the case corresponding to (b), rather than infinitely many.)

§3.4, ''Exercise 74'': If p and q are two propositions, and n a nonnegative integer, consider the compound proposition

$$r_n, \text{ defined as } \quad (\ldots((p \to q) \to q) \to \ldots) \to q, \quad \text{with } n \ q\text{'s altogether.}$$

(a) Give a recursive definition of r_n.

(b) Find the truth table of r_n for the first few values of n, conjecture a general rule, and prove this rule by induction. (Instead of stating your rule in terms of the truth table, you might list one or more short compound propositions, and prove that for each n, r_n is equivalent to one of these propositions, the choice of which one depending on n in a specified way.)

§3.4, ''Exercise 75'': (a) Let f_n denote the nth Fibonacci number. Show that for every positive integer n,

$$f_{n-1}\, f_{n+1} \; - \; f_n^2 \; = \; (-1)^n.$$

(Suggestion: Express this equation in terms of f_{n-1} and f_n only, and prove it by induction.)

(b) Prove that a positive integer a is a Fibonacci number if and only there exist positive integers b and c with $c = a + b$, such that

$$a\,b - c^2 \; = \; \pm 1$$

(i.e., such that this difference is either $+1$ or -1. Suggestion for how to approach this: Assume inductively that this statement is valid for all nonnegative integers $< a$. If b and c as above exist, you hope to show that a, b and c have the forms f_{n-1}, f_n, f_{n+1} for some n. Figure out what f_{n-2} would then have to be, verify that it, too, will satisfy such an equation, and use the inductive assumption. There are two complications: First, the term you get for f_{n-2} might not be positive. That will turn out to be a very special situation, which is easy to handle. Second, the inductive hypothesis referred to only tells you that a certain number is a Fibonacci number; but you will need to know that certain numbers are successive Fibonacci numbers. So strengthen the inductive statement that you are proving to take this into account.)

§3.5, ‘‘Exercise 45’’: Using the results of ‘‘§3.4, Exercise 66’’, give a recursive algorithm for finding the Fibonacci number f_{2^n} using $O(n)$ arithmetic operations.

§3.5, ‘‘Exercise 46’’: Give a recursive algorithm which, given an integer n and positive integers r and s both $\leq 2^n$, constructs a tiling by ‘‘L-shaped pieces’’, as discussed on pp.247-248, of a $2^n \times 2^n$ checkerboard from which the square in the rth row and sth column has been removed.

You can use for your statements of the steps of this algorithm English sentences describing things in visual terms; but the algorithm should be structured as pseudocode, and should not use expressions like ‘‘Assume without loss of generality’’ in place of case-by-case consideration.

You might, of course, like to be more thorough, and set up pseudocode which calculates the coordinates of the vertices of your L-shaped pieces, or even write code in some programming language you know that allows recursive definitions, to draw a picture of the tiling.

§3.5, ‘‘Exercise 47’’: Write a recursive algorithm which, given a polynomial $p(x)$ of degree $\leq d$, finds a polynomial $q(x)$ of degree $\leq d+1$ such that for all positive integers n one has $\Sigma_{i=1}^{n} p(i) = q(n)$. You may assume that the computer can do symbolic manipulation of polynomials, namely that it can add, subtract and multiply polynomials, substitute one polynomial into another, and give the degree and the highest-degree coefficient in a polynomial.

Suggestion: Before writing the algorithm, do the following scratchwork. Prove that $x^{d+1} - (x-1)^{d+1}$ equals a polynomial $r(x)$ of degree d, and find the coefficient c of x^d in this polynomial. Prove that $\Sigma_{i=1}^{n} r(i) = n^{d+1}$. Conclude that by subtracting an appropriate multiple of this equation from both sides of the desired equation $\Sigma_{i=1}^{n} p(i) = q(n)$, one will get a similar equation involving polynomials of lower degree. Assuming recursively that you how can find a summation formula for any polynomial of degree $< d$, can you now use this to get a solution to the original problem? Then turn these ideas into an algorithm.

§4.1, ‘‘Exercise 59’’: Find the number of bit-strings of length 100 which have the property that among every 4 successive digits, either three are 0 and one is 1, or three are 1 and one is 0.

§4.2, ‘‘Exercise 44’’: Suppose $a_1, \ldots, a_r$ is a sequence of distinct real numbers. Let i denote the length of the longest strictly increasing subsequence of this sequence, and d the length of the longest strictly decreasing subsequence, in the sense of Theorem 3, p.317.

(a) Prove an inequality (a condition expressed using ‘‘>’’, ‘‘<’’, ‘‘≥’’ or ‘‘≤’’) which must hold between i, d and r, and which is ‘‘best possible’’, in the sense that given any positive integers i, d and r that satisfy your inequality, you can construct a sequence $a_1, \ldots, a_r$ exhibiting exactly those values.

Suggestion: Examine the method of proof of Theorem 3, p.317, or of Exercise 43, p.320, and try to apply it to cases where the number of ascending and the number of descending terms you are looking for are not the same.

(b) Verify that Theorem 3, p.317, is a consequence of your result; i.e., that if $r = n^2 + 1$, then of any i and d satisfying your inequality, at least one must be $\geq n+1$.

§4.2, ‘‘Exercise 45’’: Show that there exist distinct prime numbers p_1 and p_2 such that
$$p_1 \equiv p_2 \pmod{1{,}000{,}000}.$$

§4.3, ‘‘Exercise 45’’: Suppose you want to line up a group of m men and n women for a photograph, subject to the condition that the men (ignoring the positions of the women between them) must be in increasing order of age from left to right, while the women (ignoring the positions of the men) must be in alphabetical order from right to left. In how many ways can you arrange these people that will satisfy these conditions?

§4.4, ‘‘Exercise 27(c)’’: Obtain the identity of Exercise 27 (p.334) from the identity of Theorem 4 (p.332) by a change of variables, together with an application of the identity $\binom{n}{k} = \binom{n}{n-k}$. (The latter identity is mentioned on the third line before Theorem 4, and is proved on p.323 as Corollary 1.)

§4.4, ‘‘Exercise 40’’: Give a proof by calculus of the identity of §4.4 Exercise 29, by writing the equation $(1+x)^n =$ (expansion given by the Binomial Theorem), differentiating both sides, and evaluating them at an appropriate value of x.

§4.4, ‘‘Exercise 41’’: Let us define a sequence (a_n) by the formula $a_n = \Sigma_{\substack{i+j=n \\ 0 \le j \le i}} \binom{i}{j}$, where the subscripts on the summation sign mean that the sum is over all pairs of nonnegative integers i and j which add up to n and satisfy $j \le i$ (the latter condition being needed for $\binom{i}{j}$ to be defined).

(a) Find a_n for $n = 0, \ldots, 6$. Conjecture a general formula.

(b) Prove the formula you conjectured in (a).

§4.4, ‘‘Exercise 42’’: Explore ways of extending the definition of $\binom{i}{j}$ to allow i and j to be arbitrary integers, not just nonnegative integers satisfying $i \ge j$.

(This is a very open-ended problem. It will turn out that there are ways of extending it so that some of the nice properties of the function continue to hold, and other ways of extending it so that other good properties hold, but no single way that makes all the elegant properties of that function hold. But it can be interesting to explore these extensions.)

§4.4, ‘‘Exercise 43’’: In the list of ‘‘Computations and Explorations’’ on p.353, project 3 says that it is not known ‘‘whether the largest exponent in the prime factorization of $C(2n, n)$ grows without bound as n grows’’. This condition of ‘‘growing without bound’’ might mean either of two things: That for every positive integer N there exists n such that the largest exponent in the prime factorization of $C(2n, n)$ is $\ge N$, or that for every positive integer N there exists n such that for *all* $n' \ge n$, the largest exponent in the prime factorization of $C(2n', n')$ is $\ge N$.

Determine by elimination which must be meant, by showing that one of these two questions is fairly easy to answer.

(Incidentally, in the first part of that sentence, which refers to the condition of being divisible by the square of a prime, the author presumably means ‘‘for all but finitely many n’’, since for $n = 0, 1, 2, 4$ this does not hold.)

§4.4, ‘‘Exercise 44’’: Show that given any nonnegative integers $A_1, \ldots, A_r$ and $a_1, \ldots, a_r$ such that $A_1 + a_1 = A_2 + a_2 = \ldots = A_r + a_r$, we have
$$\binom{A_1}{a_2}\binom{A_2}{a_3}\cdots\binom{A_{r-1}}{a_r}\binom{A_r}{a_1} = \binom{A_1}{a_r}\binom{A_2}{a_1}\cdots\binom{A_{r-1}}{a_{r-2}}\binom{A_r}{a_{r-1}}.$$

assuming that all the above binomial coefficients are defined (i.e., that the bottom index in each expression is $\leq$ the top index. Note that on the left side of the equation, the bottom indices are all shifted one place to the left relative to the top indices, and what would have been the leftmost index, a_1, has been brought to the far right; while on the right side, the indices are shifted one place to the right with the rightmost index, a_r, brought to the far left.)

(b) Verify that §4.4, Exercise 20 is an instance of this identity.

It would be interesting to find some combinatorial interpretation of these identities, but I can't see any.

§4.5, ''Exercise 57'': Suppose you have three flocks of chickens, with n_1, n_2 and n_3 chickens respectively, and each flock has a pecking order, from the top chicken, which can peck at any of the others, down to the bottom one which can be pecked at by all the others. Suppose you merge these into one big flock, and that this develops its own pecking order, which preserves the ordering between chickens that were originally together in a flock; i.e., such that whenever one chicken could peck at another in their original flock, it can still peck at that chicken in the combined flock.

Given the pecking orders of the old flocks, how many possibilities are there for the pecking order of the combined flock?

§4.5, ''Exercise 58'': Let n_1, n_2 and n_3 be nonnegative integers, and $n = n_1 + n_2 + n_3$.

(a) Suppose you wish to compute the coefficient of the monomial $x^{n_1} y^{n_2} z^{n_3}$ in the expansion of $(x+y+z)^n$. On the one hand, write down the formula for that coefficient given by §4.5, Exercise 53, p.344. On the other hand, apply the Binomial Theorem to $((x+y)+z)^n$ to get an expansion of this expression in powers of $x+y$ times powers of z, then argue that only one of these products (which you should specify) will, when expanded further by applying the Binomial Theorem to the power of $x+y$, give an $x^{n_1} y^{n_2} z^{n_3}$ term. Then apply the Binomial Theorem to that power of $x+y$, obtaining a formula for the coefficient of $x^{n_1} y^{n_2} z^{n_3}$.

The coefficients found by these two methods must be the same. Verify their equality directly from the formulas for these coefficients.

(b) Suppose you have $n = n_1 + n_2 + n_3$ distinguishable candies, and you want to know in how many ways you can partition them into n_1 which you will eat now, n_2 which you will eat tomorrow, and n_3 which you will give to a friend. On the one hand, give the formula for the number of ways to do this by the method of p.341. On the other hand, note that you could figure out by the method of §4.4 how many ways you can choose the n_3 to give your friend, and then how many ways to choose n_1 from those remaining, to eat now. Compare the formulas given by those two computations, and compare this comparison with that of part (a).

§4.5, ''Exercise 59'': Suppose you have $n = n_1 + n_2 + n_3 + n_4$ distinguishable objects, and you want to know in how many ways you can divide them into a set of n_1 which you will put in box 1, a set of n_2 which you will put in box 2, a set of n_3 which you will put in box 3, and a set of n_4 which you will put in box 4.

One way to do this is to first select a pile of $n_1 + n_2$ which will be divided between the two lower-numbered boxes, leaving the remaining $n_3 + n_4$ to go into the two higher-numbered boxes, and then choose, within the first pile, n_1 to go in box 1, and, within the second pile, n_3 that will go in box 3. This will determine, by elimination, where each object goes. Write down a formula for the number of ways of dividing up the n objects that this calculation gives.

On the other hand, you could first divide your objects according to whether they are to go into even- or odd-numbered boxes, and then separate out from the former pile those which will go into box 1 and from the latter those which will go into box 2, in this way again determining where each object will go. Write a formula for the number of ways you can do this.

Equating these formula gives an identity for binomial coefficients. Prove this identity directly from the definition of those coefficients.

(There are still other ways you could do this subdivision; e.g., by first choosing which objects will go into the two middle boxes; or by first choosing which should go into the first box and then subdividing the remaining ones. Comparing these, one can get still more identities.)

§4.6, ''Exercise 17'': In the paragraph before Example 5 on p.347, the author describes a way of ordering the r-combinations of the set $\{1, 2, 3, \ldots, n\}$. Since these r-combinations are subsets of $\{1, 2, 3, \ldots, n\}$, they can also be represented by length-n bit-strings (with exactly r bits equal to 1).

Describe the ordering on this set of bit-strings corresponding to the ordering of r-combinations used by the author. I.e., given two such bit-strings s and t, give a simple test that can be applied to these bit-strings to determine whether the r-combination corresponding to s or the r-combination corresponding to t comes first in that ordering, and justify your criterion.

§5.1, ''Exercise 42'': This exercise will consider the question ''What is the probability that a tossed coin shows heads n times in a row?'' If the coin is tossed exactly n times, this is easy to answer; but what if it is tossed a larger number of times?

So suppose a fair coin is tossed $n+m$ times, where n is a positive integer and m a nonnegative integer. Let E be the event that the coin comes up heads some n successive times during this series of $m+n$ tosses; i.e., that there exists a positive integer j with $j+n-1 \leq n+m$ such that the coin comes up heads on all of the jth through $j+n-1$st tosses. To dissect the different ways this can happen, let E_0 be the event that the coin comes up heads on all of the first n tosses (with no restriction on the later tosses), while for $i = 1, \ldots, m$, let E_i be the event that it comes up *tails* on the ith toss, but heads on tosses $i+1$ through $i+n$ (again, with no restriction on the results of the other tosses).

(a) Show that $E = E_0 \cup E_1 \cup \ldots \cup E_m$.

(b) Compute the values of $p(E_0)$, $p(E_1)$, $\ldots$, $p(E_m)$.

(c) Show that if $m \leq n$, then $E_0, \ldots, E_m$ are disjoint (i.e., no two of them have any elements in common).

(d) Combine the results of (a)-(c) to get a formula for the value of $p(E)$ that is valid whenever $m \leq n$.

(e) Show that the formula found in (d) can't be valid for all $m > n$, by showing that for every n there exists an m for which that formula would give a value > 1.

(f) Compute the correct value of $p(E)$ when $m = n+1$. (Hint: In that case, only one pair of the sets $E_0, \ldots, E_m$ has nonempty intersection, and that intersection is easy to describe.)

(We won't try to find a formula for $p(E)$ valid for general m in this exercise. We may do so when we get to §6.5.)

§5.1, ''Exercise 43'': Suppose as in the preceding exercise that a coin is tossed $m+n$ times, but suppose the sequence of heads and tails is written around the circumference of a circle, and let F be the event that there is a string of at least n consecutive occurrences of heads somewhere in that circle. Find and prove a formula for $p(F)$ that is correct whenever $m \leq n+1$.

§5.2, ''Exercise 39, ***continued*****'':**

(Read §5.2, Exercise 39 on p.378 of the text, then continue below.)

If $k < m$ are positive integers, let us call the results of a tournament between m players ''k-satisfactory'' if for every set of exactly k of the players, there is some player who beat them all in that tournament (the condition discussed in the second paragraph of Exercise 39).

(e) Show that for every k there exists an m such that a k-satisfactory tournament can occur among m players. (Hint: Show that for fixed k, the function $f(m) = \binom{m}{k}$ $(m \in \mathbf{N})$ can be written as a polynomial in m. Thus one factor in the inequality of part (c) has polynomial growth. How does the inverse of the other factor grow?)

(f) Try to construct, for $k = 3$ and/or 4, and some corresponding values of m, explicit k-satisfactory round-robin tournament outcomes among m players. (The smaller the value of m you can use, the better, but whether or not you get as small a value as the author's existence proof gives, it is of interest to get explicit examples.)

(g) Given natural numbers $k < m$ such that there exists a k-satisfactory tournament outcome among m players, will it be true that for any $n > m$, there also exists a k-satisfactory tournament outcome among n players?

§5.2, ''Exercise 42'': Let $m < n$ be integers, and $S = \{i \in \mathbf{Z} \mid m \leq i < n\}$, with the uniform probability distribution. Let E be the set of even integers in S, and F the set of multiples of 3 in S. Show that E and F are independent if $m \equiv n \pmod{6}$; but show by example that this may not be true if $m \not\equiv n \pmod{6}$.

§5.2, ''Exercise 43'': (a) Suppose that a box contains 2 red balls and 4 green balls. Let a ball be chosen at random, then returned to the box, and then let a ball again be chosen from the box. Let E_1 be the event that the first ball is red and E_2 the event that the second is red. Determine $p(E_1)$, $p(E_2)$ and $p(E_1 \cap E_2)$, and verify that E_1 and E_2 are independent.

(b) Suppose the above procedure is modified, in that the ball that was removed is not replaced before the second one is chosen. Let E_1 and E_2 again be the events of the first ball and the second ball being red. Compute $p(E_1)$, $p(E_2)$ and $p(E_1 \cap E_2)$ for this new situation, and verify that E_1 and E_2 are no longer independent. Give a brief conceptual explanation of the reason for this change.

Now call the box described above ''box A'', and let box B be a box with the opposite combination: 4 red balls and 2 green balls. Of course, the same results proved above also hold for the events of taking two balls from box B, with and without replacement. In particular, if we replace the first ball before making the second choice, the events of getting a red ball on the first choice and getting a red ball on the second choice are independent. However –

(c) Consider a new procedure: One of the two *boxes* is chosen at random, a ball is chosen from that box and put back in the box (as in (a)), and then a ball is again chosen from that same box. Again, let E_1 and E_2 be the events of the first ball and the second ball being red. Compute $p(E_1)$, $p(E_2)$ and $p(E_1 \cap E_2)$ for this situation. (Note: You are not asked to give different answers depending on whether box A or box B was chosen. Rather, you must take into account both the possibility that box A was used and the possibility that box B was used, each having probability .5.) Verify that here too, E_1 and E_2 are *not* independent. Again, explain briefly why this is so.

§5.2, ''Exercise 44'': Theorem 4, p.375, obtains a lower bound on the Ramsey numbers $R(k,k)$ by the probabilistic method. This exercise examines what bounds one can get similarly on the Ramsey numbers $R(2k,k)$.

[I haven't worked the steps of this exercise through myself. If you assign it, do so first!]

We start with an easy observation.

(a) For fixed k, what inequalities do we know must hold among $R(k,k)$, $R(2k,k)$, and $R(2k,2k)$? I.e., which of them must logically be $\geq$ which other(s)? Use these observations and the results of Theorem 3 to get a lower bound on $R(2k,k)$.

(b) Apply the idea of the proof of Theorem 4 in a straightforward manner to the estimation of

$R(2k,k)$. Namely, as is implicit in that proof, let S be the sample space consisting of all $2^{\binom{n}{2}}$ ways of assigning relations of friend or enemy to every pair among n people, with the uniform probability function. Let $E_1, \ldots, E_{\binom{n}{2k}}$ be the $\binom{n}{2k}$ events each of which says that one of the $2k$-person subsets of our group of n people consists of mutual friends, and $F_1, \ldots, F_{\binom{n}{k}}$ be the $\binom{n}{k}$ events each of which says that one of the k-element subsets of this group consists of mutual enemies. Then find, for given k, as large as possible a value of n for which calculations like those in the book show that the sum of the probabilities of these $\binom{n}{2k} + \binom{n}{k}$ events is <1. Note why this value of n is a lower bound for $R(2k,k)$.

(c) Repeat the calculation of part (b), this time using the probability distribution on S that assumes each pair of people has probability $2/3$ of being friends, and $1/3$ of being enemies. What lower bound does this give you for $R(2k,k)$? Is it better (i.e., stronger) or worse (weaker) than the estimate gotten in (b)?

(d) Repeat the calculation of parts (b) and (c) using the distribution under which each pair of people has probability p of being friends, and $1-p$ of being enemies, for a fixed but unspecified p. What value of p gives the best lower bound for $R(2k,k)$, and what is that bound?

§5.3, ‘‘Exercise 42’’: (a) Suppose X, Y and Z are random variables on a sample space S such that $V(X+Y) = V(X) + V(Y)$ and $V(X+Z) = V(X) + V(Z)$. Prove that $V(X+Y+Z) = V(X) + V(Y+Z)$. (You may find Exercises 36 and 37 from this section useful, though this problem can be done without them.)

(b) Give an example where the conditions of part (a) are satisfied, but where the random variables X and Y are not independent.

(c) Give an example where the conditions of part (a) are satisfied, but where $V(Y+Z)$ is not equal to $V(Y) + V(Z)$.

§5.3, ‘‘Exercise 43’’: Let e be any real number, v any positive real number, and r any positive real number such that $r^2 \geq v$. Show that there exists a sample space S with a probability function p, and a random variable X on S, such that $E(X) = e$, $V(X) = v$, and $p(|X(s)-e| \geq r) = v/r^2$; in other words, such that equality holds in Chebyshev’s Inequality with these values. (You will only need a small number of elements in S.)

Do you see why the assumption $r^2 \geq v$ is needed?

§5.3, ‘‘Exercise 44’’: Find a positive-integer-valued random variable on some sample space with finite expectation but infinite variance.

§5.3, ‘‘Exercise 45’’: Suppose X and Y are independent random variables on a probability space S.

(a) Show that for any function $f: \mathbf{R} \to \mathbf{R}$, the random variables $f(X)$ and Y are also independent.

(b) Deduce using two applications of the result of (a) that for any two functions $f, g: \mathbf{R} \to \mathbf{R}$, the random variables $f(X)$ and $g(Y)$ are independent.

In both parts (a) and (b), you may assume the sample space S is finite if you are not confident about reasoning with infinite sums.

Chapter 5, Supplementary Exercises, ‘‘Exercise 19′’’: (a) Same as part (a) of Supplementary Exercise 19 (p.396), but without the sentence about what a person should be willing to wager to play the game.

(That sentence is based on the assumption that the expected value of a game is the amount the game is ‘‘worth’’ to the player. It is based on the assumption that how much good a payoff does you is proportional to the payoff. This is reasonable for relatively small payoffs, but not for large amounts – we don’t imagine a billionaire to be a thousand times happier than a millionaire!)

In place of the second part, do:

(b) Suppose the person bankrolling this game has more than a billion but less that two billion dollars. Since 2^{30} is slightly over a billion, it is agreed that if, after the 29th flip, no head has come up, he will give the player 2^{30} dollars without doing a 30th flip, and consider the game over. What is the expected value of the game in that case?

Here is an additional part:

(c) Consider the same game, but with ‘‘2^n dollars’’ in the third line of the description replaced by ‘‘4^n dollars’’. The coin is still assumed a fair one, with probability ½ of landing heads and ½ of landing tails. How, if at all, does this change the answer to part (a)? To part (b) with ‘‘30th flip’’ replaced by the number appropriate now for the same 2^{30} dollar cap?

§5.3, ‘‘Exercise 46’’: On the middle of p.386, Rosen shows that the expectation of the number X of successive independent Bernoulli trials, each with probability p, that need to be performed before the first success occurs, is $1/p$. His proof uses an infinite summation formula which he gave without proof in the table on p.232. Here is another way of computing this expectation, *assuming it exists*, without a summation formula.

Assume that the desired expectation is a real number E. Note that if the first Bernoulli trial is a success, then $X = 1$, and this will happen with probability p, while if the first trial is a failure, then one is effectively starting over, and the number of *additional* trials needed will again have expectation E; so in this case the total expected number of trials is $1 + E$.

Combine the value of X in the first case and the expectation of X in the second, multiplying the former by the probability p that the first trial is a success and the latter by the probability $1 - p$ that it is a failure, to get a recursive expression for E in terms of itself. This is a linear equation in E; solve it for E. Compare with the value obtained on p.386.

§5.3, ‘‘Exercise 47’’: (a) Again suppose a series of independent Bernoulli trials, each with probability p of success, is performed, but this time suppose one waits till one sees *two successive* successes; i.e., two successes in a row, with no failure between them. Find the expected number of trials that must be performed for this to happen, as a function of p. (Suggestion: Divide into three cases: Two successes at the start, an initial success followed by a failure, and an initial failure, and use the idea of the preceding exercise.)

(b) Similarly, find the expected number of trials that must be performed if one is waiting till one sees a success followed immediately by a failure. (Hint: If the first trial is a success, observe that what you are looking for will occur at the very first failure thereafter. Use the result of ‘‘Exercise 46’’ above, with success and failure interchanged, to find the expected number of steps before this happens. On the other hand, treat the case where the first trial is a failure as in part (a).)

(c) Deduce from the results of (a) and (b) the expected number of trials needed in the cases where one waits instead for two successive failures, or a failure followed immediately by a success.

§5.3, ‘‘Exercise 48’’: Assume n independent Bernoulli trials, each with probability p of success, is performed.

(a) Determine the expected number of cases of two successive successes occurring in these n trials, the expected number of cases of a success followed immediately by a failure, the expected number of cases of a failure followed immediately by a success, and the expected number of cases of two successive failures. (Note: In a sequence like SFFSSSSF, we count three cases of two successive successes: trials (4,5), (5,6) and (6,7), despite the fact that these overlap.)

(b) Verify that if $p = 0.5$, then the expected numbers of occurrences of the above four patterns, as computed in part (a), are equal; but that the expected numbers of trials until the patterns first occur, computed in the preceding exercise, are not all equal. I leave you to think about this paradox.

§6.1, ''Exercise 69'': This exercise is related to the ideas of ''§5.3, Exercises 46-48'' above, but does not require that you have done those exercises.

Suppose a series of independent Bernoulli trials, is performed, each with probability p of success and hence probability $q = 1-p$ of failure.

(a) For each integer $n \geq 2$, let E_n be the event that the nth trial is the first time one has gotten two successive successes; meaning that the $n-1$st and nth trials are both successes, but no case of two successes in a row happens earlier. Find a recurrence relation satisfied by the numbers $p(E_n)$.

(Idea: Suppose $n \geq 4$. If the first trial is unsuccessful, then E_n means that among the next $n-1$ trials, two successive successes occur for the first time at the very end. If the first trial is successful, then for E_n to occur, we must have failure on the second step, and then have two successive successes occur for the first time as of the $n-2$nd step after those two. Use these facts, and the known probabilities of success and failure in the first trial, to express $p(E_n)$ in terms of $p(E_{n-1})$ and $p(E_{n-2})$.)

(b) For $p = ½$, calculate $p(E_2)$ and $p(E_3)$ directly, and using these and the recurrence relation found in part (a), find $p(E_4)$, $p(E_5)$ and $p(E_6)$.

(c) Continuing to assume $p = ½$, conjecture, based on the results of part (b), a general formula for $p(E_n)$, and prove your formula by mathematical induction.

(Hint: The powers of 2 occurring in the denominators of the probabilities found in part (b) will be somewhat irregular. Whenever the power is lower than expected, multiply numerator and denominator by an appropriate factor to bring it up, so that the denominators form a straightforward sequence, and then look at the numerators.)

(d)-(f) For each integer $n \geq 2$, let F_n be the event that the nth trial is the first time one has gotten a success followed immediately by a failure; meaning that the $n-1$st trial is a success, the nth trial is a failure, and no such pattern has occurred earlier. Use methods like those of parts (a)-(c) to obtain a general formula for $p(F_n)$ when $p = ½$.

§6.4, ''Exercise 61'': (a) Suppose the sequence $a_0, a_1, \ldots$ satisfies the homogeneous linear recurrence relation

$$a_n \;=\; c\,a_{n-1} + d\,a_{n-2} \qquad (n \geq 2).$$

Let $f(x) = \Sigma_{k=0}^{\infty} a_k x^k$. Show that $(1 - cx - dx^2)\, f(x)$ is a polynomial, i.e., has only finitely many nonzero terms. Express this polynomial using c, d, and the initial terms a_0 and a_1 of the given sequence. Deduce from this result an expression for $f(x)$ as a rational function, i.e., a polynomial divided by another polynomial.

(This embraces the essence of Rosen's subsection ''Using generating functions to solve recurrence relations'', pp.444-446. The same thing works for linear recurrence relations of any degree; I just didn't want to overload you with details.)

(b) Deduce a closed-form expression for the generating function of the sequence of Fibonacci numbers.

(c) Get a different closed form expression for the generating function of the Fibonacci numbers by taking the expression for f_n found in Example 4, p.416, substituting it into the definition of the generating function, and breaking the resulting power series into two power series having geometric progressions for coefficients, each of which you can express in closed form.

(d) Show how the expression gotten in (c) can be simplified to give the expression gotten in (b).

(e) Show that every finite bit-string without two consecutive zeroes can be obtained in one and only one way by stringing together substrings of the forms ‘‘1’’ and ‘‘10’’, and then removing the first digit, which has to be a ‘‘1’’, from the resulting string.

Hence every bit-string of length n without two consecutive zeroes can be obtained uniquely by stringing together ‘‘1’’s and ‘‘10’’s whose lengths add up to $n+1$, and removing the first ‘‘1’’. Now

(f) Using the method of Example 12, pp.441-442 in the case where ‘‘the order of tokens matters’’, find the generating function for the number of bit-strings of length n obtainable by stringing together ‘‘1’’s and ‘‘10’’s. Making use of part (e) above, and of the remark on p.407, end of Example 6, relate this generating function to that of the Fibonacci numbers, and so obtain the formula for that function in yet another way.

§6.4, ‘‘Exercise 62’’: (a) For the situation of ‘‘§6.1, Exercise 69(a)-(c)’’, compute the generating function $\Sigma_{k=0}^{\infty}\, p(E_k)\, x^k$ by combining the result of that exercise with the calculation of ‘‘§6.4, Exercise 61(a)’’ above.

If you have done §6.4, Exercise 57, you can go on to do

(b) Use the result of part (a) and the formula for the expectation of an integer-valued random variable in terms of its generating function to compute the same number asked for in ‘‘§5.3, Exercise 47(a)’’.

(c)-(d) Do the same for the generating function $\Sigma_{k=0}^{\infty}\, p(F_n)$ of ‘‘§6.1, Exercise 69(d)-(f)’’ and the expectation asked for in ‘‘§5.3, Exercise 47(b)’’.

§6.4, ‘‘Exercise 63’’: (a) Let S be a finite set, let $f: S \to \mathbf{R}$ be any real-valued function on S, and for any subset T of S, let $w(T) = \Sigma_{s \in T}\, f(s)$. (We may think of this as the ‘‘weight’’ of T.)

Show that if $A_1,\ A_2, \ldots, A_n$ are subsets of S, then

$$w(A_1 \cup \ldots \cup A_n) \;=\; \Sigma_{1 \le i \le n}\, w(A_i) \;-\; \Sigma_{1 \le i < j \le n}\, w(A_i \cap A_j)$$
$$+\;\Sigma_{1 \le i < j < k \le n}\, w(A_i \cap A_j \cap A_k) \;-\; \ldots \;+\; (-1)^{n+1}\, w(A_1 \cap \ldots \cap A_n).$$

(Suggestion: Use a method of proof is analogous to that of Theorem 1 of this section.)

(b) Show that both Theorem 1 of this section and the result of Exercise 23, p.457 can be obtained as special cases of the result of part (a) above.

(In part (a), I assume S finite to avoid questions of convergence of infinite sums. If the correct assumptions are made about these, the results is true without the finiteness assumption. In applying this result to get that of Exercise 23, assume the sample space in that exercise is finite.)

§6.4, ‘‘Exercise 64’’: (a) Give an alternative version of proof of Theorem 1, p.454, based on the following idea: After beginning as in the first two sentences of that proof, choose any k such that $a \in A_k$. Now consider those nonempty subsets $U = \{i_1, \ldots, i_m\} \subseteq \{1, \ldots, n\}$ such that $a \in A_{i_1} \cap \ldots \cap A_{i_m}$. In general, one can pair each subset U of this sort that does not contain k with the subset $U \cup \{k\}$ which does. Verify that the contributions of these two sets to the formula of Theorem 1 cancel each other. Note, however, that there is one nonempty subset $U \subseteq \{1, \ldots, n\}$ for which the associated intersection of A_is contains a but which is not paired in this way with any other. What is it? Taking this into account, conclude that a is counted exactly once.

(b) Let $1 < r < n$, and suppose that in the right-hand side of the formula of Theorem 1 we only add up the first r terms; i.e., those based on intersections of $\le r$ sets. Show that in place of the indicated equality, one can deduce an inequality, with a ‘‘$\le$’’ relation if n is odd (i.e., if the first of the terms we have dropped had a minus sign) and a ‘‘≥’’ relation if n is even (if the first term we have dropped had a plus sign).

§6.5, ‘‘Exercise 30’’: (a) Find the number of nonnegative integers less than 1,000,000 which are not divisible by any of 2, 3, 5 or 11.

(b) Find a formula which, for every positive integer n, gives the number of nonnegative integers less than $330n$ which are not divisible by any of 2, 3, 5 or 11.

(Since 1,000,000 is not a multiple of 330, part (b) does not have part (a) as a special case. Being a multiple of 330 makes part (b) particularly easy.)

§6.5, ‘‘Exercise 31’’: Applying the result of Rosen’s Exercise 23, p.457, and its generalization to k events, to the situations of parts (e) and (f) of ‘‘§5.1, Exercise 42’’, extend the results of those parts beyond the cases $m = n$ and $m = n+1$. (It will be easy to get the next few cases. I haven’t examined whether there will be a nice general formula that can be proved for all m.)

Similarly, extend the result of ‘‘§5.1, Exercise 43’’.

§7.1, ‘‘Exercise 58’’: Let A be a set, and $\mathrm{Rel}(A)$ the set of all binary relations on A. We see that given any $R, S \in \mathrm{Rel}(A)$, their composite $R \circ S$ will also be a member of $\mathrm{Rel}(A)$.

(a) Is the operation of composition on $\mathrm{Rel}(A)$ associative? I.e., is it true that for all $R, S, T \in \mathrm{Rel}(A)$ one has $(R \circ S) \circ T = R \circ (S \circ T)$?

(b) Is the operation of composition on $\mathrm{Rel}(A)$ commutative? I.e., is it true that for all $R, S \in \mathrm{Rel}(A)$ one has $R \circ S = S \circ R$?

(c) Is the operation of composition on $\mathrm{Rel}(A)$ distributive with respect to union? I.e., is it true that for all $R, S, T \in \mathrm{Rel}(A)$ one has $R \circ (S \cup T) = (R \circ S) \cup (R \circ T)$ and $(R \cup S) \circ T = (R \circ T) \cup (S \circ T)$?

(d) Is the operation of composition on $\mathrm{Rel}(A)$ distributive with respect to intersection? I.e., is it true that for all $R, S, T \in \mathrm{Rel}(A)$ one has $R \circ (S \cap T) = (R \circ S) \cap (R \circ T)$ and $(R \cap S) \circ T = (R \circ T) \cap (S \circ T)$?

On p.480, before Exercise 24, the author defines the *inverse* R^{-1} of a relation R from a set A to a set B. In particular, if $R \in \mathrm{Rel}(A)$ (the case $A = B$ of that definition) then $R^{-1} \in \mathrm{Rel}(A)$ as well.

(e) Given $R, S \in \mathrm{Rel}(A)$, is $(R \circ S)^{-1}$ equal to the composite, in one or the other order, of R^{-1} and S^{-1}?

§7.2, ‘‘Exercise 30’’: (a) Let R be the ternary (i.e., 3-ary) relation on $\mathbf{Z}$, $\mathbf{Z}$ and $\mathbf{Z}^+$ consisting of all 3-tuples (a, b, m) such that $a \equiv b \pmod{m}$. Show that R has no primary keys, and no composite keys except for the whole set $\mathbf{Z} \times \mathbf{Z} \times \mathbf{Z}^+$.

(b) Let R' be the ternary relation on $\mathbf{Z}$, $\mathbf{Z}$ and $\mathbf{Z}^+$ consisting of all 3-tuples (a, b, m) such that $a = b \,\mathbf{mod}\, m$. Show that R' again has no primary keys, but that it does have a composite key consisting of the cartesian product of two of the three domains.

§7.4, ‘‘Exercise 36’’: Let R be a relation on a set S, let G be its directed graph, and let n be a positive integer.

(a) Show that G has at least one circuit of length n if and only if the directed graph corresponding to R^n has at least one loop.

(b) What can one say about the relationship between the number of circuits of length n in G and the number of loops in the directed graph corresponding to R^n? (Must they always be equal? If not, can we bound one or both in terms of the other?)

§7.5, ‘‘Exercise 56’’: Let R be an equivalence relation on a set A, let C be the set of all equivalence classes of A with respect to R, and let $f: A \to B$ be any function. Show that the following conditions are equivalent:

(i) There exists a function $g: C \to B$ such that for every $a \in A$ one has $g([a]_R) = f(a)$.

(ii) For all $(a, b) \in R$, $f(a) = f(b)$.

Show also that when these equivalent conditions are satisfied, the function g referred to in (i) is unique.

Remark: It is common in mathematics to define a function g on a set of equivalence classes by a formula like the final equation of (i). (Examples are given in parts (a) and (c) of the next exercise.) The verification that this procedure actually determines a function is called ‘‘showing that g is well-defined’’, and consists in checking condition (ii). The set of equivalence classes of A with respect to R, which I have denoted C here, is most often written A/R.

§7.5, ‘‘Exercise 57’’: Let m be a positive integer and let R be the relation on $\mathbf{Z}$ consisting of $\{(a, b) \mid a \equiv b \pmod m\}$. The set of equivalence classes of R will be denoted $\mathbf{Z}_m$.

(a) Show with the help of the preceding exercise that there is a unique function $g: \mathbf{Z}_m \to \mathbf{Z}_m$ such that $g([a]_R) = [a^2]_R$ for all $a \in \mathbf{Z}$. (That is, ‘‘squaring mod m is well-defined’’.)

(b) Show for some m that there is no $g: \mathbf{Z}_m \to \mathbf{Z}_m$ such that $g([a]_R) = [2^a]_R$ for all $a \in \mathbf{Z}^+$. (‘‘Base-2 exponentiation mod m is not well-defined’’.)

(c) Show that there exists a unique function $g: \mathbf{Z}_m \to \mathbf{Z}$ such that $g([a]_R) = a \ \mathbf{mod}\ m$ for all $a \in \mathbf{Z}$. Verify that this function is one-to-one.

Remark: A more general version of the result of the exercise preceding this one can be verified for functions of one or more variables, allowing one to show easily that, for example, ‘‘addition mod m’’ and ‘‘multiplication mod m’’ are well-defined.

§7.5, ‘‘Exercise 58’’: Show that if A and B are two sets having the same number of elements, then the number of equivalence relations on A and the number of equivalence relations on B are the same.

(If this seems obvious to you, then good – you have the right intuition. But one needs to learn how to give the logical argument that supports such intuition.)

§7.6, ‘‘Exercise 52(b)’’: Let S be the set of strings described in Exercise 52, and S' the subset of S consisting of those strings *not* ending in the letter a. Show that $(S', \preccurlyeq)$ *is* a dense poset.

§7.6, ‘‘Exercise 60’’: (a) Show that if $(S, \preccurlyeq)$ is a finite poset, and $a \in S$, then a is the greatest element of S if and only if it is the *only* maximal element of S. (So in particular, S has a greatest element if and only if it has a unique maximal element.)

(b) Show that if S is not assumed finite, then one of the implications expressed by the ‘‘if and only if’’ of part (a) remains true, but the other is false. (To show the falsity of that statement, you must give a counterexample.)

Note that the results corresponding to (a) and (b) are also true with ‘‘least’’ and ‘‘minimal’’ in place of ‘‘greatest’’ and ‘‘maximal’’, by corresponding arguments and examples.

(c) Show that if $(S, \preccurlyeq)$ is a *well founded* poset, in the sense of the paragraph before Exercise 49, p.530, then it is again true that an element a is the least element of S if and only if it is the unique minimal element of S.

§7.6, ‘‘Exercise 61’’: Let $(S, \preccurlyeq)$ be a poset. What does it mean for an element $a \in S$ to be a least upper bound of the empty subset $\varnothing$ of S? A greatest lower bound of $\varnothing$ in S?

§7.6, ‘‘Exercise 62’’: If $(S, \preccurlyeq)$ is a finite poset, one defines the *height* of S to be the greatest integer n such that there exist elements $a_1, \dots, a_n \in S$ such that $a_1 \prec \dots \prec a_n$, and the *width* of S to be the greatest integer n such that there exist elements $a_1, \dots, a_n \in S$ no two of which are comparable. (A family of elements of the first sort is called a *chain* in S and a family of the second sort, an *antichain*.) Denoting these values by $\mathrm{ht}(S)$ and $\mathrm{wi}(S)$, show that

$$|S| \ \leq \ \mathrm{ht}(S) \cdot \mathrm{wi}(S).$$

(One way to do this is with the help of Supplementary Exercise 32, p.534, but this would require doing that difficult exercise. There is an easier method.)

§7.6, ‘‘Exercise 63’’: A relation $\preccurlyeq$ on a set S which is reflexive and transitive (but not necessarily antisymmetric) is called a *preordering*. In particular, note that every partial ordering is a preordering, and every equivalence relation is also a preordering. A pair $(S, \preccurlyeq)$ where $\preccurlyeq$ is a preordering on S is often called a *preordered set* or simply a *preorder*. Here are a couple of examples of preorderings other than partial orderings and equivalence relations:

(a) Rosen observes that the relation of divisibility on $\mathbf{Z}^+$ is a partial ordering. Show that the relation of divisibility on the whole set $\mathbf{Z}$ is a preordering, but not a partial ordering.

(b) Suppose that $f: S \to T$ is any function, and let $\preccurlyeq_T$ be any partial ordering on T. Define a relation $\preccurlyeq_S$ on S by letting $a \preccurlyeq_S b$ for $a, b \in S$ if and only if $f(a) \preccurlyeq_T f(b)$. Show that $\preccurlyeq_S$ is a preordering on S, but that if f is not one-to-one, this preordering will not be a partial ordering.

In the remaining three parts, $\preccurlyeq$ will be any preordering on any set S. Given $a, b \in S$, let us define $a \approx b$ to mean $(a \preccurlyeq b) \wedge (b \preccurlyeq a)$.

(c) Show that $\approx$ is an equivalence relation on S.

Following the notation of Definition 2, p.509, let us denote the equivalence class under $\approx$ of an element $a \in S$ by $[a]_\approx$. Let S' denote the set of all such equivalence classes. Given $[a]_\approx$, $[b]_\approx \in S'$, let us write $[a]_\approx \preccurlyeq' [b]_\approx$ if $a \preccurlyeq b$ in S.

(d) Show that the relation $\preccurlyeq'$ is *well-defined*, i.e., that for $s, t \in S'$, the above criterion gives the same answer as to whether $s \preccurlyeq' t$ holds, regardless which $a \in A$ such that $s = [a]_\approx$ and which $b \in A$ such that $t = [b]_\approx$ we choose.

(e) Show that the relation $\preccurlyeq'$ is a partial ordering on S'.

§7.6, ‘‘Exercise 64’’: Suppose $(S, \preccurlyeq)$ is a finite poset, and T is the set of all total orderings ‘‘$\leq$’’ on S which are compatible with $\preccurlyeq$, in the sense defined on p.525 just before Lemma 1. (So I am writing ‘‘$\preccurlyeq$’’ where that definition used R, and ‘‘$\leq$’’ where that definition used ‘‘$\preccurlyeq$’’. In doing this exercise, if you want to refer to different elements of T, I suggest you call them $\leq_1$, $\leq_2$ etc..) Let us put the uniform probability distribution on T. Thus, for $s, t \in S$, the expression $p(s \leq t)$ denotes fraction of the elements $\leq \in T$ for which $s \leq t$ holds; i.e.,

$$p(s \leq t) \ = \ |\{\leq \in T \mid s \leq t\}| \,/\, |T|.$$

(a) Show that elements $s, t \in S$ are incomparable if and only if $0 < p(s \leq t) < 1$.

(b) *Open question in the theory of finite posets.* Is it true that whenever S is not totally ordered, there exist $s, t \in S$ such that $1/3 \leq p(s \leq t) < 2/3$?

Some examples you might like to examine in thinking about this question are

(i) The 3-element poset with Hasse diagram , and

(ii) For $n \geq 3$, the poset whose elements are $1, \dots, n$, and where we define $i \preccurlyeq j$ to hold if and only if either $i = j$ or $j - i \geq 2$ (with ‘‘$\geq$’’ having the usual meaning for real numbers).

You may wonder why the above question is of interest. Well, suppose we have a set S of n objects, on which some total ordering $\leq$ is given, where we do not this ordering, but can test any two of these objects and determine which is the larger under the ordering. (E.g., we may have n stones of slightly different weights, and a balance with the help of which we can find which of any two stones is the heavier.) How many tests do we have to make to determine the total ordering $\leq$?

There are $n!$ possibilities for that ordering. It would be nice if with each test we could cut the number of possibilities for $\leq$ in half; we could then be sure of determining $\leq$ in $\log(n!)$ tries. Since for $n > 2$, $n!$ is not a power of 2, we cannot precisely do this; but can we get close?

After any sequence of tests, we know from those tests the relations among certain of the objects. Now if we know that $a \leq b$ and that $b \leq c$ then we certainly know that $a \leq c$. Hence if we write $a \preccurlyeq b$ whenever $a \leq b$ follows logically from the results of the tests we have made, then the relation $\preccurlyeq$ is transitive. It is easy to see that it is also reflexive and antisymmetric, so $\preccurlyeq$ is a partial ordering on S. The linearizations of this partial ordering constitute the set of possibilities for the ordering $\leq$ consistent with the results of the tests we have made.

So it is natural to ask whether, on reaching a given such situation, we can make tests in such a way that each test cuts the set of linearizations of $\approx$ *nearly equally* in two. Example (i) above shows that in the worst cases we can't do better than cut it in a two-to-one ratio. If we can even be sure that we can always do that, then starting with no information we can find our original ordering in $\lfloor \log_{3/2}(n!) \rfloor$ tries. This is the motivation for the open problem.

Of course, this analysis ignores the possibility that by some strategy of testing we may be able to avoid having to deal frequently (or at all) with worst-case partial orderings. How good a strategy of this sort one can find is also an interesting question! However, I hope that the above discussion does give some interest to the open question described.

§8.1, ''Exercise 30'': (a) Draw the simple graph whose vertices are the integers $0, 1, \ldots, 9$, and whose edge-set consists of those pairs $\{u, v\}$ such that $u \equiv v \pmod 3$.

(b) Draw the directed graph whose vertices are the integers $0, 1, \ldots, 9$, and whose edge-set consists of those pairs (u, v) such that $u \mid v$.

(c) Draw the directed graph whose vertices are the integers $0, 1, \ldots, 5$, and whose edge-set consists of those pairs (u, v) such that $v = u+1$.

(d) Draw the directed graph whose vertices are the integers $0, 1, \ldots, 5$, and whose edge-set consists of those pairs (u, v) such that $v \equiv u+1 \pmod 6$.

Appendix A-2, ''Exercise 4'': What will be the effect of the following block of statements, applied to numbers x and y?

$x := x + y$
$y := x - y$
$x := x - y$

This gives an interesting alternative solution to Exercise 2 of this Appendix – but only for the case where the values of x and y are numbers. It would obviously be of no help if x and y were airlines, movies you wanted to see, ingredients in a recipe, etc..

Appendix A-2, ''Exercise 5'': What is the value of n when the following program halts?

procedure *doubleawhile*
$n := 1$
while $n < 100$
    $n := 2n$