

1. a) Determine which of the following propositions are tautologies. Show why.

$$(p \rightarrow \neg q) \rightarrow (\neg q \rightarrow p)$$

Not a tautology. Take p and q to be false; then $p \rightarrow \neg q$ is true but $\neg q \rightarrow p$ is false.

$$[(p \vee q) \rightarrow r] \leftrightarrow [(p \rightarrow r) \wedge (q \rightarrow r)]$$

Tautology:

$$\begin{aligned} (p \vee q) \rightarrow r &\Leftrightarrow \neg(p \vee q) \vee r \\ &\Leftrightarrow (\neg p \wedge \neg q) \vee r \\ &\Leftrightarrow (\neg p \vee r) \wedge (\neg q \vee r) \\ &\Leftrightarrow (p \rightarrow r) \wedge (q \rightarrow r) \end{aligned}$$

b) Write down a proposition P over the variables p, q, r such that P is true only when p, q, r have truth values FFT or TFT .

$$P \Leftrightarrow (\neg p \wedge \neg q \wedge r) \vee (p \wedge \neg q \wedge r) \Leftrightarrow \neg q \wedge r$$

c) Can such a P be constructed using the connectives \wedge and \rightarrow only (no truth constants for T and F are allowed)? If yes, do so. Otherwise show why not.

No: Note that P is false when $p, q,$ and r are all true. Since $\mathbf{T} \wedge \mathbf{T} \Leftrightarrow \mathbf{T}$ and $\mathbf{T} \rightarrow \mathbf{T} \Leftrightarrow \mathbf{T}$, any formula built only from \wedge and \rightarrow will be true when the atoms $p, q,$ and r are all true, and you need it to be false!

[Reminder: you weren't allowed to use \neg in part c.]

2. a) Let $L(x, y)$ be x loves y . Write the following as formal sentences with quantifiers

Everybody	loves	somebody	$\forall x \exists y L(x, y)$
Everybody	loves	everybody	$\forall x \forall y L(x, y)$
Somebody	loves	everyone	$\exists x \forall y L(x, y)$
Somebody	loves	someone	$\exists x \exists y L(x, y)$

b) Which of the following sentences are logically equivalent (answer only)? In principle you have to determine the equivalence of all 6 pairs of sentences.

1) $\forall x(A(x) \rightarrow B)$, 2) $\forall x A(x) \rightarrow B$, 3) $\exists x(A(x) \rightarrow B)$, 4) $\exists x A(x) \rightarrow B$.

(B does not contain x .)

We have $1 \Leftrightarrow 4$ and $2 \Leftrightarrow 3$ (directly from Handout #2).

To see that (1) and (2) are not logically equivalent, let the universe of discourse be \mathbb{Z} , let B be \mathbf{F} , and let $A(x)$ be $x = 0$. Then $\forall x A(x)$ is false, since $\neg A(1)$; so (2) is true. (1) is false, however, since $A(0)$ is true but B is false.

Since \Leftrightarrow is an equivalence relation, it follows immediately that $1 \not\Leftrightarrow 3$, $4 \not\Leftrightarrow 2$, and $4 \not\Leftrightarrow 3$. [If we had $1 \Leftrightarrow 3$, for example, then we would be able to get $3 \Leftrightarrow 2$ (symmetry) and then $1 \Leftrightarrow 2$ (transitivity).]

3. Which of the following are always true (A, B, C are arbitrary sets)? Yes-No answers.

if $A \subseteq B$ and $B \subseteq A$ then $A = B$	Y
$\emptyset \in \{\emptyset\}$	Y
$\emptyset \in A$	N (consider $A = \{1, 2\}$)
$\emptyset \subseteq A$	Y
if $A \neq B$ and $B \neq C$ then $A \neq C$	N (take $A = C = \emptyset$ and $B = \{1\}$)
$A - B = \overline{(\overline{A} - \overline{B})}$	N (if $A = B$ then $\overline{A} - \overline{B} = \emptyset = A - B$)
$(A - B) \cap (B - A) = \emptyset$	Y
$\emptyset \times A = \emptyset$	Y
$A \times B = B \times A$	N
$\overline{A \cup B} = \overline{A} \cup \overline{B}$	N

4. How many one-to-one functions f from $\{1, 2, 3, 4, 5\}$ onto itself are there such that $f \circ f \circ f$ is the identity function?

As usual, the first step is to understand the objects that we're counting; a useful and elegant tool for understanding permutations is the concept of an "orbit" of an element in the domain.

The orbit of an element x is just the set of elements that you would generate if you started with x and then successively applied f ; i.e., it's the set

$$\{x, f(x), f^2(x), f^3(x), f^4(x), f^5(x), \dots\} = \{f^i(x) \mid i \geq 0\}.$$

In this exercise, $f^3(x) = x$ is a given, so x 's orbit collapses down to $\{x, f(x), f^2(x)\}$,

$$\{f^i(x) \mid i \geq 0\} = \{f^{i \bmod 3}(x) \mid i \geq 0\} = \{f^0(x), f^1(x), f^2(x)\} = \{x, f(x), f^2(x)\},$$

and it may collapse further, depending on x . Orbits are nice combinatorially because their internal structure is simple and because they partition the domain. [Partition: x , $f(x)$, and $f^2(x)$ clearly all have the same orbit, since

$$\{x, f(x), f^2(x)\} = \{f(x), f^2(x), x\} = \{f^2(x), x, f(x)\}.$$

In other words, if y appears in an orbit O , then y 's own orbit coincides with O .]

What more can we say about these orbits? Clearly, it's possible that $f(x) = x$, in which case x 's orbit is the singleton set $\{x\}$ and x is said to be a "fixpoint." What else might happen?

Could x 's orbit collapse to $\{x, f(x)\}$, with $f(x) \neq x$? No, since that would mean that either $x = f(f(x))$, which would imply $f(x) = f(f(f(x))) = x$, or $f(x) = f(f(x))$, which would imply $x = f(x)$ since f is invertible [$f^{-1} = f^2$]. An orbit of size 2 would thus be inconsistent with $f^3(x) = x$.

An orbit of size 3,



a.k.a. a "3-cycle," would be ok, though, since applying f^3 , which corresponds to taking three steps around the 3-cycle, would always bring you back to your starting point.

We just showed that, if $f \circ f \circ f$ is the identity function, then, for every x in its domain, either x is a fixpoint or x is part of a 3-cycle. In fact, this condition on the orbits is both necessary and sufficient for $f \circ f \circ f$ to be the identity function. [Sufficiency: taking three steps around a 3-cycle always brings you back to your starting point, and a fixpoint never "moves" anywhere.]

Thus, we just need to count the number of permutations of $\{1, 2, 3, 4, 5\}$ that satisfy the “fixpoints and 3-cycles” condition. Now, there are only 5 elements in the domain, so there’s room for at most one 3-cycle. This means that we can conveniently partition the set of f ’s into two disjoint subsets: “subset 0,” permutations with no 3-cycles, and “subset 1,” permutations with exactly one 3-cycle.

If f is in “subset 0,” then every element is a fixpoint, i.e., $f(x) = x$ for every x . Thus, there is really only one function (the identity function) in subset 0.

If f is in “subset 1,” then it has exactly one 3-cycle and exactly two fixpoints. First, choose the two fixpoints [$C(5, 2)$ ways to do that]. Then, choose a 3-cycle on the remaining three elements, exactly like seating 3 guests around a circular table [$(3 - 1)!$ ways to do that—see question 11c]. Using the product rule, there are thus $C(5, 2)(3 - 1)!$ functions in subset 1.

The two subsets are disjoint, by design, so we can now apply the sum rule to get

$$1 + C(5, 2)(3 - 1)! = 21$$

as the total number of functions.

[Addendum: the equation $f^i = f^{i \bmod 3}$ can be justified by the derivation $f^{3k+r} = f^{3k} \circ f^r = (f^3)^k \circ f^r = (\text{id})^k \circ f^r = \text{id} \circ f^r = f^r$, where id denotes the identity function.]

5. Yes-No answers. Is it true that n^2 is $O(g(n))$, if $g(n)$ is

n	N
n^3	Y
$n \log n$	N
2^n	Y
$n!$	Y
$n^2 \log n$	Y
$n^2 + \log n$	Y
$n^2 / \log n$	N
$(n^4 + 1)/(n^2 + 1)$	Y
$(n^4 + 1)/(n + 1)$	Y

6. Find $5^{20001} \pmod{143}$. The answer should be a standard integer between 0 and 143.

Note that $143 = 11 \cdot 13$ is not prime, so we can't directly apply Fermat's Little Theorem. (In fact, $5^{142} \pmod{143} = 25 \neq 1$.) We can, however, first use Fermat's Little Theorem to compute the related quantities $5^{20001} \pmod{11}$ and $5^{20001} \pmod{13}$ and then combine those results via the Chinese Remainder Theorem.

In detail: since 5 is relatively prime to both 11 and 13, and since 11 and 13 are both prime, we can safely apply Fermat's Little Theorem to get the congruences $5^{10} \equiv 1 \pmod{11}$ and $5^{12} \equiv 1 \pmod{13}$. From there,

$$5^{20001} \equiv 5^1 \cdot (5^{10})^{2000} \equiv 5 \pmod{11}$$

and

$$5^{20001} \equiv 5^9 \cdot (5^{12})^{1666} \equiv 5^9 \pmod{13}$$

Little trick: $5^2 \equiv 25 \equiv 12 \equiv -1 \pmod{13}$, so $5^9 \equiv 5 \cdot (5^2)^4 \equiv 5 \pmod{13}$.

Thus, 5^{20001} and 5 are congruent both mod 11 and mod 13. By the uniqueness clause of the Chinese Remainder Theorem, this implies that 5^{20001} and 5 are also congruent mod 143. [11 and 13 are relatively prime, so this application of the Chinese Remainder Theorem was legitimate.]

7. a) Perform the following operations on binary numbers:

$$1101 + 1011 = 11000$$

$$1101 \cdot 1011 = 10001111$$

$$1101/1011 = (\text{find a quotient and a remainder})$$

$$1101 = 1011 \cdot 1 + 10$$

b) Transform $(1101)_2$ into decimal. $1 + 0 + 4 + 8 = 13$

c) Transform $(1101)_{10}$ into binary. $1101 = 1024 + 64 + 8 + 4 + 1 = (10001001101)_2$

8. a) Give an example of matrices A and B such that $AB \neq BA$.

Take $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$; then $AB = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $BA = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.

b) Find all 2×2 zero-one matrices whose boolean square is the zero matrix. The answer only.

$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, and $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$.

[A matrix with a 1 in one of the diagonal entries cannot work, and the boolean square of $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is the identity matrix.]

c) How many integer additions and how many integer multiplications does it take to multiply two 5×5 integer matrices using the standard row-column algorithm (answer only)?

It takes $5 \cdot 5 \cdot 5 = 125$ multiplications and $5 \cdot 5 \cdot 4 = 100$ additions.

9. a) Suppose that $S(n)$ is a proposition involving a nonnegative integer n , and suppose that if $S(k)$ is true then so is $S(k+2)$. Which of the following are possible (answer only)?

$S(n)$ holds for all $n \geq 0$, Y

$S(n)$ holds for all $n \geq 1$, but $S(0)$ is false, Y

$S(n)$ is false for all $n \geq 0$, Y

$S(n)$ is true for all $n \leq 100$ and false for all $n > 100$, N

$S(n)$ is false for all $n \leq 100$ and true for all $n > 100$. Y

[In the above, “Y” means “possible,” and “N” means “not possible.”]

b) A collection S of strings of characters is defined recursively by

i) the empty string is in S , ii) if X belongs to S then so does aXb .

Which of the following belong to S (Yes-No answers):

a N

b N

c N

ab Y

abb N

$aabb$ Y

10. a) A questionnaire is sent to 13 freshmen, 5 sophomores, 15 juniors, and 20 seniors. A student won't necessarily return his/her questionnaire. How many questionnaires must be received to ensure getting 9 from the same class?

We could receive 5 from sophomores, 8 from freshmen, 8 from juniors, and 8 from seniors and still not meet the condition. One more, and we'd be ok.

So, $5 + 8 + 8 + 8 + 1 = 30$.

b) How many bit strings are there of length 10 with two or more 1's in the string?

[Leading 0's are ok.]

There are 2^{10} strings of length 10. Among them, $C(10, 0) = 1$ have no 1's, and $C(10, 1) = 10$ have exactly one 1.

$$N = 2^{10} - 1 - 10 = 1013$$

11. a) Find the number of positive integer solutions of $x + y + z \leq 100$.

First, we use the standard technique for converting a \leq problem into an $=$ problem: it suffices to find the number of nonnegative integer solutions of $x + y + z + e = 100$, subject to the constraint $x \geq 1 \wedge y \geq 1 \wedge z \geq 1$.

Next, we use the standard technique for dealing with \geq constraints: we just need to find the number of nonnegative integers solutions of $x' + y' + z' + e = 100 - 1 - 1 - 1 = 97$.

Finally, using "stars and bars," we get $C(97 + 4 - 1, 4 - 1) = C(100, 3)$.

[Recall that the \leq technique works because there is a one-to-one correspondence between the triples (x, y, z) that satisfy $x + y + z \leq 100$ and the quadruples (x, y, z, e) that satisfy $x + y + z + e = 100$; simply map $(x, y, z) \mapsto (x, y, z, 100 - x - y - z)$. The inverse, $(x, y, z, e) \mapsto (x, y, z)$, works because $x + y + z = 100 - e \wedge e \geq 0$ ensures $x + y + z \leq 100$.]

b) A hostess wishes to invite 6 dinner guests. In how many ways can she place them on 6 distinguished seats?

There are $6! = 720$ possible ways.

c) The same question for a round table with indistinguishable seats.

Decide the position of the first guest. You then have 5 places left.

There are $5! = 120$ possibilities.

12. Two fair dice are rolled. What is the probability that

a) the number on the first die is strictly less than the number on the second die?

There are $\sum_{i=1}^6 \sum_{j=1}^{i-1} 1 = \sum_{i=1}^6 (i-1) = 0 + 1 + 2 + 3 + 4 + 5 = 15$ relevant outcomes, each of which has probability $\frac{1}{36}$. (In the double summation, i is the number on the second die, and j is the number on the first die.)

$$P = \frac{15}{36} = \frac{5}{12}$$

b) one of those numbers is strictly less than the other one?

This fails only when the two numbers are equal, and there are exactly six outcomes in which the two numbers are the same.

$$P = 1 - \frac{6}{36} = \frac{5}{6}$$

c) the product of those numbers is even given that their sum equals 6 ?

The outcomes in which the sum is 6 are

$$(1, 5), (5, 1), \underline{(2, 4)}, \underline{(4, 2)}, (3, 3)$$

and we can easily prove that this list is complete by quickly calculating the number of positive integer solutions to $i + j = 6$: $C((6-1-1) + 2 - 1, 2 - 1) = C(5, 1) = 5$.

The two underlined outcomes are the ones in which the product is even. Thus,

$$P = \frac{2}{5}$$

13. A couple agrees to keep having children until they have at least one boy and one girl, but not more than 5 children. Assume that boys and girls are equiprobable and that the births are mutually independent. What is the expected value and variance of the number of

a) children ? b) girls ?

The sample space is

outcome	BG	GB	BBG	GGB	BBBG	GGGB	BBBBG	GGGGB	BBBBB	GGGGG
prob.	1/4	1/4	1/8	1/8	1/16	1/16	1/32	1/32	1/32	1/32

Let Y be the number of boys and let X be the number of girls. Then

$$E(X + Y) = 2 \cdot \left(\frac{1}{4} + \frac{1}{4}\right) + 3 \cdot \left(\frac{1}{8} + \frac{1}{8}\right) + 4 \cdot \left(\frac{1}{16} + \frac{1}{16}\right) + 5 \cdot \left(\frac{1}{32} + \frac{1}{32} + \frac{1}{32} + \frac{1}{32}\right) = \frac{23}{8}$$

Likewise,

$$E((X + Y)^2) = 2^2 \cdot \left(\frac{1}{4} + \frac{1}{4}\right) + 3^2 \cdot \left(\frac{1}{8} + \frac{1}{8}\right) + 4^2 \cdot \left(\frac{1}{16} + \frac{1}{16}\right) + 5^2 \cdot \left(\frac{1}{32} + \frac{1}{32} + \frac{1}{32} + \frac{1}{32}\right) = \frac{75}{8}$$

The variance of $X + Y$ is thus $E((X + Y)^2) - (E(X + Y))^2 = \frac{71}{64}$.

Now, by symmetry, $E(X) = E(Y)$, so $E(X + Y) = E(X) + E(Y) = 2E(X)$, whence $E(X) = \frac{1}{2}E(X + Y) = \frac{23}{16}$. Also,

$$E(X^2) = 0^2 \cdot \frac{1}{32} + 1^2 \cdot \left(\frac{1}{4} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \frac{1}{32}\right) + 2^2 \cdot \frac{1}{8} + 3^2 \cdot \frac{1}{16} + 4^2 \cdot \frac{1}{32} + 5^2 \cdot \frac{1}{32} = \frac{98}{32}$$

The variance of X is thus $E(X^2) - (E(X))^2 = \frac{255}{256}$.

14. An integer is randomly selected from 1 to 1000. What is the probability that it is divisible by 2 or by 3 or by 5?

Let A be the event “divisible by 2,” let B be the event “divisible by 3,” and let C be the event “divisible by 5.” Inclusion-exclusion yields

$$P(A \cup B \cup C) = P(A) + P(B) + P(C) - P(A \cap B) - P(A \cap C) - P(B \cap C) + P(A \cap B \cap C)$$

and the terms on the right-hand side are

$$\begin{aligned} P(A) &= \lfloor 1000/2 \rfloor / 1000 = 500/1000 \\ P(B) &= \lfloor 1000/3 \rfloor / 1000 = 333/1000 \\ P(C) &= \lfloor 1000/5 \rfloor / 1000 = 200/1000 \\ P(A \cap B) &= \lfloor 1000/6 \rfloor / 1000 = 166/1000 \\ P(A \cap C) &= \lfloor 1000/10 \rfloor / 1000 = 100/1000 \\ P(B \cap C) &= \lfloor 1000/15 \rfloor / 1000 = 66/1000 \\ P(A \cap B \cap C) &= \lfloor 1000/30 \rfloor / 1000 = 33/1000 \end{aligned}$$

Thus, $P(A \cup B \cup C) = (500 + 333 + 200 - 166 - 100 - 66 + 33)/1000 = 734/1000$.

15. Give an example of a relation R that is

a) symmetric, not reflexive

$x R y \Leftrightarrow x = -y$, over the domain \mathbb{Z} .

This is not reflexive: $1 R 1$ does not hold (since $1 \neq -1$).

b) reflexive, symmetric, not transitive.

$x R y \Leftrightarrow |x - y| \leq 1$, over the domain \mathbb{Z} .

This is not transitive: $1 R 2$ and $2 R 3$ but $\neg(1 R 3)$.

16. a) How many vertices and edges does the graph Q_5 have?

Recall that Q_5 is the 5-dimensional hypercube, a graph that has 2^5 vertices, each of degree 5. Using the handshaking theorem, the number of edges is $\frac{1}{2}(2^5 \cdot 5) = 2^4 \cdot 5 = 80$.

b) A graph has 7 vertices, 3 of them of degree two and 4 of degree one. Is this graph connected? Why?



Not connected—by the handshaking theorem, this graph has only $\frac{1}{2}(3 \cdot 2 + 4 \cdot 1) = 5 < 6$ edges, so it cannot have a spanning tree.

(Recall that a spanning tree of an n -vertex graph is just an n -vertex subgraph that is a tree. It's easy to see that every connected, undirected graph has a spanning tree [just run BFS, starting at an arbitrary node]. In general, an n -vertex tree has exactly $n - 1$ edges, so every connected, n -vertex graph has at least that many edges.)

17. Which of the following graphs have an Euler circuit? An Euler path? (Answer only)

K_5	circuit & path	... all vertices have degree 4
Q_3	neither	... all vertices have degree 3
Q_4	circuit & path	... all vertices have degree 4
$K_{2,5}$	path only	... 2 of degree 5, 5 of degree 2
$K_{3,5}$	neither	... 3 of degree 5, 5 of degree 3

18. Which of the following graphs are planar? (Answer only)

K_5	not planar	... K_5 is a subgraph
Q_3	planar	... can be drawn as 
$K_{2,5}$	planar	... can be drawn as 
$K_{3,5}$	not planar	... $K_{3,3}$ is a subgraph
$K_{4,5}$	not planar	... $K_{3,3}$ is a subgraph