Math 55 — Discrete Mathematics — Spring 2003

Review Problems for Final Exam

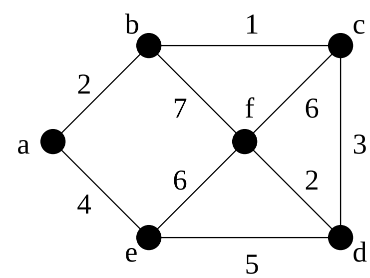
The final examination is Wednesday, May 21, 8:00–11:00 AM in Room 10, Evans Hall. Please arrive a few minutes early to make it easier to get everyone seated and hand out the exams.

No books, notes or calculators may be used. Bring scratch paper.

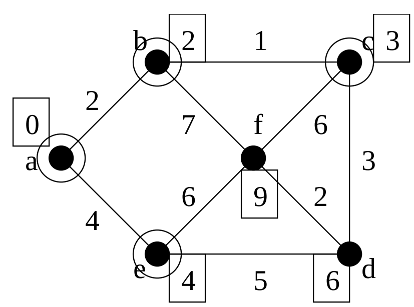
The exam will cover material from the whole semester, with more emphasis on material from after the second midterm exam.

The review problems below should give a fair idea of the subject matter and level of difficulty of the exam.

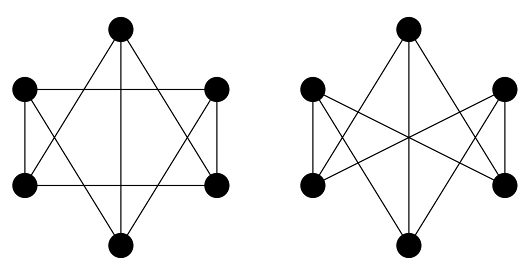
1. In the graph shown below, with edge lengths as indicated, find:
   (a) the length of the shortest path from vertex a to each of the other vertices;
   (b) the shortest path from vertex a to vertex f.



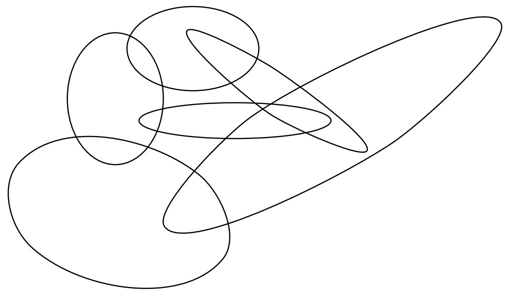
2. For the graph in problem 1, Dijkstra's algorithm after four steps finds the neighborhood $\{a, b, c, e\}$ of vertex a, with distance labels as shown in the rectangular boxes below. Which vertex gets added to the neighborhood at the next step, and what are the new labels afterwards?



3. Either exhibit an isomorphism between the two graphs shown below, or prove that none exists.



4. Let G be the graph whose vertices are the ovals the figure below, with edges representing pairs of ovals that overlap. Write down an adjacency matrix for G, and draw a picture of G with vertices and edges shown in the usual way.



5. Prove that a graph with 9 vertices and 14 edges must have a vertex of degree at least 4.

6. Suppose that each pair of people in a group are either friends, enemies or strangers. Prove that if there are 17 people in the group then there are either three mutual friends, three mutual enemies, or three mutual strangers.

7. How many ways are there to assign 8 different tasks to 12 workers if each worker can only do one task? What if each worker can do more than one task?

8. Prove the identity

$$\binom{n}{j, k, n-j-k} = \binom{n}{j}\binom{n-j}{k}$$

(a) algebraically, and (b) combinatorially.

9. How many different graphs are there with 10 edges and vertex set $\{1, 2, 3, 4, 5, 6, 7, 8\}$? In this problem, graphs count as different if they have different edges, even if they are isomorphic.

10. How many possible selections of two dozen jelly beans are there if they come in 5 flavors: cherry, lemon, chocolate, blueberry, and mint? How many if you dislike mint and will not take more than three mint jelly beans?

11. How many 7-permutations of the 26 letters of the alphabet contain the letters A, B, C
   (a) in order, but not necessarily consecutively?
   (b) in order and consecutively?

12. Find all the smaller lists that get merged at every level of recursion when the merge-sort algorithm is used to sort the list of integers

$$(9, 4, 5, 2, 12, 10, 7, 8, 6, 11, 3, 1)$$

13. Let f_k denote the k-th fibonacci number. Prove that

$$f_1 + f_3 + \cdots + f_{2n-1} = f_{2n}$$

for every positive integer n.

14. What is wrong with this "proof" that all horses are the same color?

Let $P(n)$ be the proposition that in every set of n horses, all the horses are the same color. We will prove $P(n)$ by induction on n.

Basis step: Clearly, $P(1)$ is true.

Induction step: For $n > 1$, let $\{H_1, \dots, H_n\}$ be a set of n horses. Since $\{H_1, \dots, H_{n-1}\}$ is a set of $n-1$ horses, we may assume by induction that horses H_1 through H_{n-1} are all the same color. Since $\{H_2, \dots, H_n\}$ is also a set of $n-1$ horses, we may further assume that horses H_2 through H_n are all the same color. Therefore horse H_n is the same color as horses H_1 through H_{n-1}, and all the horses in our set are the same color.

15. (a) Let p/q be a rational number, $0 < p/q < 1$. Show that if n is the smallest positive integer such that $1/n \leq p/q$, then $(p/q) - (1/n)$ is either equal to zero or to a rational number p'/q' with $p' < p$.

(b) Use part (a) and strong induction on p to prove that every rational number p/q with $0 < p/q < 1$ can be expressed as a sum of one or more fractions of the form $1/n$. (For example, $\frac{13}{15} = \frac{1}{2} + \frac{1}{3} + \frac{1}{30}$.)

16. For the 3-error correcting Reed-Solomon code over $\mathbb{Z}_{11}$ with 4 message symbols and 10 code symbols, determine whether each of the two vectors below is a code vector or not.

$$\text{(a)} \qquad \begin{bmatrix} 2 & 3 & 3 & 1 & 7 & 9 & 6 & 8 & 3 & 1 \end{bmatrix}$$

$$\text{(b)} \qquad \begin{bmatrix} 2 & 3 & 4 & 6 & 7 & 9 & 0 & 8 & 3 & 1 \end{bmatrix}$$

17. Consider the linear code over $\mathbb{Z}_2$ with 4 message bits, 8 code bits, and code matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

(a) How many errors can this code correct?
(b) How many errors can it detect?

18. Find all solutions of the system of equations

$$\begin{aligned} 4x + 2y + 3z &\equiv 2 \pmod 5 \\ 3x - 2y - z &\equiv 4 \pmod 5 \end{aligned}$$

19. Find all solutions of the system of equations

$$\begin{aligned} x &\equiv 3 \pmod 5 \\ x &\equiv 1 \pmod 7 \\ x &\equiv 3 \pmod{11} \end{aligned}$$

For the next two problems you will need a calculator. Exam questions on these topics will not require one.

20. Consider the RSA cryptosystem with public key

$$\begin{aligned} n &= 572149, \\ e &= 5. \end{aligned}$$

(a) Encrypt the message $x = 339412$ using this cryptosystem.
(b) Given the prime factorization $n = 727 \cdot 787$, find the decryption key for this cryptosystem.

21. Use Pollard's "tail-chasing" method to find the prime factorization of n in the previous problem without knowing it in advance.

22. Apply Fermat's test to $n = 35$, first using the base 6, then using the base 7. What can be deduced from the result of each test about whether 35 is prime or composite, without using other information?

23. Repeat the previous problem using Miller's test instead of Fermat's test.

24. Solve the congruence $7x \equiv 11 \pmod{26}$.

25. Use Fermat's little theorem to find the inverse of $5 \pmod{17}$.

26. Find all solutions of the congruence $x^2 \equiv 16 \pmod{105}$. Note that $105 = 3 \cdot 5 \cdot 7$.

27. Prove that $\log_2(3)$ is irrational. Hint: if $\log_2(3) = p/q$, then $2^p = 3^q$.

28. Determine whether each of the following functions is $O(n^2)$, $\Omega(n^2)$, $\Theta(n^2)$, or none of these.
(a) $f(n) = \binom{n}{2}$
(b) $f(n) = n \log n$
(c) $f(n) = n^2 \log n$
(d) $f(n) = \begin{cases} n^3 & \text{if } n \text{ is odd} \\ 0 & \text{if } n \text{ is even} \end{cases}$