Institut for Matematik og Datalogi
Syddansk Universitet

Exam Assignment 1
Algorithms and Probability — 2018

This is the first of two sets of problems (assignments) which together with the oral exam in January constitute the exam in DM551. This first set of problems may be solved in groups of up to three.

The assignment is due at 12:15 on Monday, October 22. You may write this either in Danish or English. Write your full name (or names if you do it together — up to three people may work together) clearly on the first page of your assignment (on the top, if it's not a cover page). Turn it in as a PDF file via Blackboard through your DM551 course. The assignment hand-in is in the menu for the course and is called "SDU Assignment". Keep the receipt it gives you proving that you turned your assignment in on time. Blackboard will not allow you to turn in an assignment late.

Cheating on this assignment is viewed as cheating on an exam. Do not talk with anyone outside of your group (or Kristine Knudsen or Joan Boyar) about the assignment, and do not show your solutions to anyone outside your group. If you have questions about the assignment, come to Joan Boyar or Kristine Knudsen.

Assignment 1

Do the following problems. Write clear, complete answers, but not longer than necessary. Explain all answers, especially those where the answer is just a number.

1. Suppose there are at least $n \geq 2$ people in a room. Assume that for any two people in the room, they either both know each other, or neither knows the other. Prove that there are at least two people in the room who know the same number of people.

2. What is the coefficient of x^{95} in the expansion of $(x+3)^{189}$? Explain how you got this answer. (Do not reduce to an actual integer.)

3. Prove: **Theorem:** For any $n \in \mathbb{N}$ the number of odd entries in row n of Pascal's triangle is 2 raised to the power equal to the number of ones in the binary expansion of n.

   To prove this result, first try to prove the following:

   - Show that for any positive integers $k < 2^i$ and $t < i$, 2^t divides k if and only if 2^t divides $2^i - k$.
   - $$(1+x)^{2^i} \bmod 2 = 1 + \mathrm{x}^{2^\mathrm{i}} \bmod 2 \ \forall \mathrm{i} \in \mathbb{N} \ .$$

     Here, taking a polynomial $(1+x)^{2^i}$ modulo 2 means to take its coefficients modulo 2. The above statement says that all coefficients of $(1+x)^{2^i}$ except the first and the last are even.

   Next, use this result for computing the number of odd coefficients in $(1+x)^n$ for an arbitrary n by considering its binary expansion

   $$n = \sum_{i=0}^{s} b_i \cdot 2^i \ .$$

4. Choose a random letter x from the string "THEOREM" and a random letter y from the string "COROLLARY". What is the probability that $x = y$? Explain your answer.

5. A bakery has 5 types of cupcakes: chocolate with cream cheese frosting, chocolate with chocolate frosting, carrot, banana nut, and apple/cinnamon. How many ways are there to choose:

   (a) 6 cupcakes?

   (b) 10 cupcakes with at least one of each type of cupcake?

6. What is the next permutation of the set $\{1, 2, 3, 4, 5, 6, 7, 8\}$, in ascending lexicographic order, after the permutation 12857643?

7. How would you you change Algorithm 1, in Section 6.6 of Rosen's textbook, to produce the previous instead of the next permutation (for the purpose of producing the sequences in reverse lexicographic order, starting from $n, n-1, ..., 2, 1$)? Give a complete algorithm, but explain where it is different from Algorithm 1.

8. Suppose that three fair dice are rolled. What are the following:
   (a) the probability that the sum of the three numbers is at least 15?
   (b) the expected number of times that three dice need to be rolled before the sum of the three numbers is at least 15?
   (c) the probability that the sum of the three numbers is at least 15, given that the first of the three dice has value 5? (Explain how you computed this using conditional probabilities.)

9. Consider Example 16 on page 450 in Rosen's textbook, on probabilistic primality testing. Given the information there, for any given composite integer $n > 1$, give an upper bound on the expected number of iterations of Miller's test before n fails the test?

10. Design and analyze a Monte Carlo algorithm to determine if two polynomials, $f(x)$ and $g(x)$, are equal to each other. Assume that the only access you have to the two polynomials is through two procedures F and G, which each have exactly one integer argument x, where F computes $f(x)$ and G computes $g(x)$. Thus, you could compute both f and g on the value 3 by running $F(3)$ and $G(3)$. If two polynomials both have degree at most k ($x^4 - 5x^3 - 2x + 9$ has degree 4, the highest exponent on x), then if they are the same on more than k different values, they are identical. Assume that you have a large upper bound n on the degrees of f and g, but the bound is so large that you cannot try $n+1$ different values. State explicitly which values you are choosing randomly among, and compute the probably of error, assuming that the polynomials both have degree n (for both possible answers your algorithm can give).

11. Consider rolling a fair die.
    (a) What is the exact probability that either a 1 or a 6 is rolled?
    (b) Use Chebyshev's inequality to give an upper bound on the probability that you roll either a 1 or a 6.
    (c) Use Markov's inequality to give an upper bound on the probability that you roll a 6.

12. Find the number of positive integers not exceeding 100 that are not divisible by 2, 3, 5, or 7.

13. How many solutions does $x_1 + x_2 + x_3 = 15$ have where x_1, x_2, and x_3 are nonnegative integers less than or equal to 6? (Use the principle of inclusion-exclusion.)

14. Suppose that p and q are odd primes with $p \neq q$ and s is a positive integer. Use the principle of inclusion-exclusion to compute $\phi(p^s q)$, the number of positive integers less than $p^s q$ which are not divisible by p or q (are relatively prime to $p^s q$).