Mathematical Foundations of Computer Science

Ten Powerful Ideas

and applications

Final Exam	Bruce Maggs	May 4, 1998

NAME :

ANDREW ID :

SECTION : A B C D

INSTRUCTIONS. WRITE CLEARLY. WRITE YOUR NAME AND ANDREW ID ABOVE AND CIRCLE YOUR SECTION.

Repeat After Me.

This part is to test your ability to study material and repeat it.

1. [3 points] **Contrapositive.**
What is the contrapositive of the assertion "A implies B"?

2. [3 points] **Geometric series.**
Give a closed-form expression for $\sum_{i=0}^{+\infty} x^i$, where $|x| < 1$.

3. [3 points] **Group size.**
State *Lagrange's Theorem.*

4. [3 points] **Polynomial interpolation.**
In the finite field GF_p, how many degree-$(n-1)$ polynomials pass through the k points $(x_1, y_1), (x_2, y_2), (x_3, y_3), \ldots, (x_k, y_k)$? (Assume $k \leq n$.)

5. [3 points] **One-to-one function.**
Let f be a function from a set A to a set B. Give a necessary and sufficient condition for f to be a *one-to-one* function.

6. [3 points] **The halting problem.**
Give an example of a real number that is describable but not computable.

7. [3 points] **Finite probability space.**
Suppose that Ω is a finite set of *outcomes* and that p is a function from subsets of Ω (called *events*) to real numbers in the range $[0, 1]$. What two conditions must p satisfy in order for Ω and p together to form a probability space?

8. [3 points] **Fermat's Little Theorem.**
State *Fermat's Little Theorem.*

9. [3 points] **Big-Omega notation.**
Suppose that f and g are both functions from the natural numbers to the natural numbers. Give a precise definition of the notation $f(n) = \Omega(g(n))$.

10. [3 points] **Field.**
The following definition of a field has one mistake in it. What is the mistake? A set S together with an addition operator $\oplus$ and a multiplication operator $\odot$ form a *field* if S and $\oplus$ form a commuative group, S and $\odot$ form a commutative group, and $\odot$ distributes over $\oplus$.

11. [5 points] **Horner's method.**
Suppose that the n coefficients of a degree $n-1$ polynomial $p(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0$ are stored in an array a, so that the coefficient of x^i in $p(x)$ is $a[i]$. Write a piece of C or C++ code to evaluate p at some point $x = b$, i.e., evaluate $p(b)$. Ignoring calculations of loop indices, your program must perform at most $n-1$ additions and $n-1$ multiplications.

12. [5 points] **Euclid's algorithm.**
Given two non-negative integers a and b, where $b \geq a$, Euclid's algorithm finds the greatest common divisor of a and b. Give a short recursive description of Euclid's algorithm (in pseudocode or C/C++).

Basic Techniques.

This part will test your ability to reason with some of the basic techniques learned in the class.

13. [8 points] **Recurring nightmares.**
Give a closed-form solution to the following recurrence. Show your work.

$$
\begin{aligned}
f(n) &= 5f(n-2) - 4f(n-4) \\
f(0) &= 2 \\
f(1) &= 0 \\
f(2) &= 8 \\
f(3) &= 0
\end{aligned}
$$

14. [8 points] **Seven-card stud.**
Seven-card stud is a variation of poker in which each player is dealt seven cards, and then selects any five of the seven to form a poker hand.

How many times more likely is it to receive a hand containing four-of-a-kind in seven-card stud than in the version of poker in which each player is dealt five cards and cannot discard or exchange any cards? (We're looking for the ratio of the probabilities.)

15. [8 points] **Even worse than taking this final.**
Four graders have 112 final exams to grade.

1. (4 points) How many different ways are there of dividing up the 112 exams among the 4 graders? (We don't care if some graders get more work than others.)

2. (4 points) Suppose that the graders are not concerned with the names of the students on the exams that they are to grade, but only about the number of exams that they are to grade. How many different ways are there of partitioning the exams when they are all indistinguishable (again, not caring if some graders get more work than others)?

A Moment's Thought!

This section tests your ability to think a little bit more insightfully. You must give complete explanations of your answers. **Do three of the five problems. Do not do all five; if you do we will grade three of our choice.**

16. [12 points] **We really do think like this.**
Prof. Baraff and Prof. Maggs are competing to see who can give harder homework assignments. For each assignment, Prof. Maggs wins with probability 1/2 and Prof. Baraff wins with probability 1/2, independent of the outcomes of the previous assignments. The competition ends when one of these (admittedly somewhat evil) professors has won on two more of the assignments than the other one. At this point the professors stop giving out assignments. How many 15-299 assignments do you expect to have to do?

Hint: Look at two assignments at a time.

17. [12 points] **Defying all expectations.**
Provide a counterexample to the following hypothesis.

Hypothesis. For every finite probability space and every random variable x defined on that probability space, for any function f mapping the reals to the reals,

$$E[f(x)] = f(E[x]).$$

Give a counterexample (a random variable x and a function f that falsify the hypothesis) and show why.

18. [12 points] **Sign on the dotted line.**
In the RSA public-key cryptography system, a plaintext message m from Bob to Alice is encrypted using Alice's public key $\langle e, n\rangle$ by computing $m^e \bmod n$. Alice, who has a private key d such that $e \cdot d = 1 \bmod \phi(n)$, then decrypts the message by computing $(m^e)^d = m^{ed} = m \bmod n$.

One drawback to the scheme, as described so far, is that there is no way for Alice to tell if the message really was sent by Bob, or if it was forged by an imposter. To remedy this problem, a signature scheme is used. Suppose that Bob's public key is $\langle e', n'\rangle$, and his private key is d', such that $e' \cdot d' = 1 \bmod \phi(n')$. Rather than sending m^e to Alice, Bob sends $(m^{d'} \bmod n')^e \bmod n$.

1. (4 points) Explain how Alice recovers the original plaintext message m.

2. (4 points) Why can Bob be confident that revealing both m and $m^{d'} \bmod n'$ to Alice is a safe thing to do? *Hint: How can Alice generate a similar pair of numbers x and $x^{d'} \bmod n'$ by herself, using only public information?*

3. (4 points) Why is Alice confident that the message $(m^{d'}) \bmod n'$ was encrypted by Bob and not by someone else?

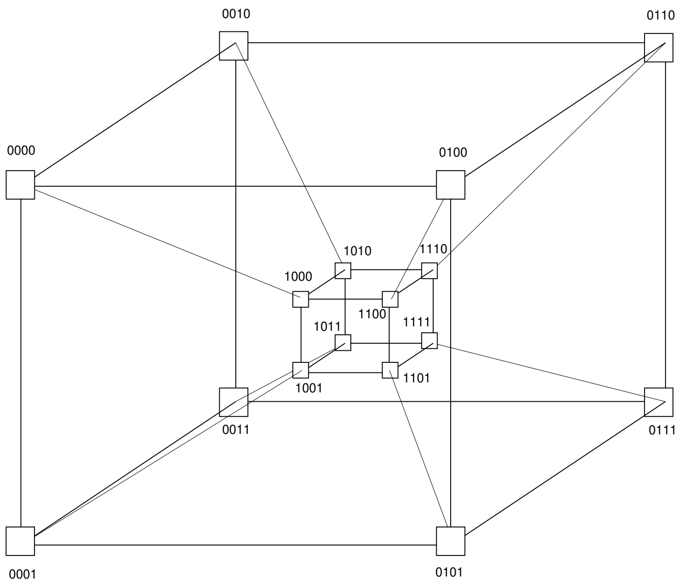
19. [12 points] **That's irrational.**
A real number is called *rational* if it can be expressed as the ratio of two integers, and *irrational* otherwise. In solving this problem, you may assume that $\sqrt{2}$ is irrational. (It is.)

1. (4 points) Prove that if x is a rational number, then $x \cdot \sqrt{2}$ is an irrational number.

2. (4 points) Let Q denote the set of rational numbers, and let T denote the set of numbers that are rational multiples of $\sqrt{2}$, i.e., $T = \{y : y = x \cdot \sqrt{2},\ x \in Q\}$. Prove that there is a one-to-one and onto mapping from $Q \cup T$ to T.

3. (4 points) Prove that the set of real numbers has the same cardinality as the set of irrational numbers. *Hint: divide the real numbers into* $Q \cup T$ *and* $\mathcal{R} - (Q \cup T)$.

20. [12 points] **Hypercubic.**
The *hypercube* of dimension k, abbreviated H_k, is a graph that can be constructed recursively by making two copies of H_{k-1} and joining corresponding nodes in the two copies by an edge. For the base case, H_0 is a single node. The hypercube H_4 is shown below.



1. (6 points) Prove by induction that H_k has $k2^{k-1}$ edges.

2. (6 points) Prove that for all $k \geq 2$, H_k has a Hamiltonian tour. (Recall that a *Hamiltonian tour* is a simple cycle that visits all of the nodes in a graph.)

And now for the revelation that you've all been waiting for ... "What the heck is APE 0835?" My license plate!