Mathematics Masters Examination

Option 4

March 29, 2005

Computer Science

2:5 PM

Note: Any student whose answers require clarification may be required to submit to an
oral examination.

Each of the twelve numbered questions is worth 20 points. All questions will be graded, but
your score for the examination will be the sum of your scores on your eight best questions.

Please observe the following:

- **Do not** answer two or more questions on the same sheet
  (not even on both sides of the same sheet).

- **Do not** write your name on any of your answer sheets.

You will be given separate instructions on the use of these answer sheets. When you have
completed a question, place it in the large envelope provided.
Computer Algorithms

1. Describe an $O(n)$-time algorithm that, given points $x_1 < x_2 < \cdots < x_n$ on the real line, determines the smallest set of unit-length closed intervals that contains all the given points. Make sure to argue that your algorithm is correct.

2. Someone proposes the following divide-and-conquer algorithm for computing minimum spanning trees. Given a weighted graph $G = (V, E)$, partition $V$ into two sets $V_1$ and $V_2$ such that $|V_1|$ and $|V_2|$ differ by at most 1. For $i = 1, 2$, let $E_i$ be the set of edges that are incident only on vertices in $V_i$. Recursively solve the minimum-spanning-tree problem on each of $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$. Finally, select a minimum-weight edge in $E$ that crosses $V_1$ and $V_2$, and use this edge to unite two minimum spanning trees into a single spanning tree.

For each $n$ large enough, give a weighted graph $G$ on $n$ vertices for which the algorithm fails.

Combinatorics

3. (a) How many nonequivalent ways are there to color the vertices of the regular 10-gon with three colors Red, Blue, and Green? As usual, equivalence is with respect to all symmetries of the 10-gon, i.e., rotations and reflections.

(b) How many of the colorings in (a) have exactly 4 Red, 4 Blue and 2 Green vertices?

4. Suppose we have $n$ employees in a company, and wish to form committees of these employees. Suppose we are not allowed to have a committee all of whose members are also in another committee. Determine the maximum number of committees we can have. Give an example to show how to achieve this number of committees. (For example, if $n = 3$, we could choose committees $\{a, b\}, \{a, c\}, \{b, c\}$ or we could choose committees $\{a\}, \{b\}, \{c\}$; in fact, it is not hard to see that the maximum number of committees one can choose is 3 when $n = 3$).

Graph Theory

5. Show that if $G$ is a connected graph with two or more vertices, then at least two vertices of $G$ are not cut-vertices.

6. (a) State Hall’s Theorem on matchings in bipartite graphs.

(b) Use (a) to prove that for $k \geq 1$, every $k$-regular bipartite graph has a perfect matching.

Error-Correcting Codes and Cryptography

7. Is the ternary code with the following parity-check matrix perfect? Give reasons.

$$H = \begin{pmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 1 & 2 \end{pmatrix}$$

Spring 05 CS 2/4
8. Alice wants to receive RSA-encrypted messages. She chooses two primes $p = 7$ and $q = 11$, which she keeps secret, and computes $n = pq = 77$. She also chooses an encryption exponent $e = 53$. Alice’s public key is $(n, e)$.

(a) What is Alice’s private key, and how does she compute it? For full credit, use a method of computation that would be practical (with a computer) even if $p$ and $q$ were 200-digit primes instead of 1 or 2-digit primes.

(b) Bob sends Alice a message (consisting of an integer in the range $[0, 76]$) encrypted using her public key. The encrypted message is 3. How does Alice decrypt the message, and what was the original message? Again, for full credit, use a method of computation that would be practical even if $p$ and $q$ were 200-digit primes.

(c) Eve intercepts Bob’s encrypted message, and easily decrypts it. Would Eve be able to decrypt the message if Alice had chosen 200-digit primes $p$ and $q$ (avoiding some bad cases)? Why or why not?

Theory of Computation

9. Recall that a string $w$ is a prefix of a string $u$ if $u = wx$ for some string $x$. For a language $L$, let

$$\text{Pref}(L) = \{ w \mid \text{for some } u \in L, \text{ w is a prefix of } u \}$$

be the set of prefixes of strings in $L$. Show that if $L$ is regular, then $\text{Pref}(L)$ is also regular.

10. Is the language

$$L = \{ a^nb^mc^{n+2} \mid n, m \geq 0 \}$$

context-free? Justify your answer.

Numerical Analysis

11. Using Newton's Method, find a numerical approximation to the Intersection of $\exp(0.1969 + x)$ and $7.471/x$ on $[3.0, 4.0]$ starting with the endpoint and $k = 1$ having the smallest value of $|f|$, keeping track of the number of ALL function evaluations $k_{fe}$, and tabulating

| $k$ | $k_{fe}$ | $x_k$ | $f_k$ | $f'_k$ | $x_{k+1}$ | $|\Delta x_k|$ |
|-----|----------|-------|-------|--------|-----------|---------|
| 1   |          |       |       |        |           |         |
| 2   |          |       |       |        |           |         |
| :   |          |       |       |        |           |         |
| 4   |          |       |       |        |           |         |

until $|\Delta x_k| = |x_{k+1} - x_k| < 0.5e-4$ and $|f_k| < 0.5e-4$, or else use $k_{max} = 4$. 

Spring 05 CS  3/4
12. Using **Forward Gaussian Elimination** with **Virtual Partial Pivoting, Virtual Row Scaling,** and **Back Substitution,** solve the following algebraic system for the vector $\bar{x} = [x_1]_{3 \times 1}$,

$$-6.657 \cdot x_1 - 10.66 \cdot x_2 + 7.542 \cdot x_3 = 46.89$$

$$7.745 \cdot x_1 + 3.865 \cdot x_2 + 4.062 \cdot x_3 = 80.58$$

$$0.5643 \cdot x_1 + 7.583 \cdot x_2 - 2.704 \cdot x_3 = 57.56$$

Record **Augmented Matrices** with **Marked Multipliers, Pivot Vectors, Scale Vectors** and **scratch work**, i.e., $[A \mid \bar{b} \parallel \bar{P} \parallel \bar{S} \parallel \text{scratch} ]$, at each elimination step, including the initial step (note the scratch item is the absolute value of the potential pivot divided by its row scaling). Compute the relative residual of the approximate solution as the ratio of infinity-norms, but also give the values of the residual vector and the norms used.
1. **Algorithm:** Starting from \( x_1 \), draw an unit-interval \( I_1 = [x_1, x_1 + 1] \). Then start from the first \( x_i \) which is outside \( I_1 \) and draw \( I_2 = [x_i, x_i + 1] \), etc. An iterative code is easy to write (as in Page 378) and I skip it here (it is enough to write English sentences for the credits of this part).

**Cost:** since we scan each point once, this greedy algorithm takes only \( O(n) \)-time.

**Proof:** we prove the correctness of the algorithm above by showing that \( I_1 = [x_1, x_1 + 1] \) is contained in some minimal interval cover. Let \( A = \{J_1, J_2, \ldots, J_m\} \) be a minimal interval cover (\( J_i \) are intervals of length 1) and suppose \( x_1 \in J_1 \). If \( J_1 \) is same as \( I_1 \), we are done. Otherwise let \( A' = A - J_1 + I_1 \) and we claim that \( A' \) is also a minimal interval cover. In fact, since no point is on the left of \( x_1 \) and all \( x_j \) included in \( J_1 \) are not greater than \( x_1 + 1 \), the new interval \( I_1 \) covers all the \( x_j \) included in \( J_1 \). Hence \( A' \) is also a cover (and minimal as well).

2. An easy example is that \( G \) is a complete graph on \( n \) vertices with \( V(G) = V_1 + V_2 \), such that \( ||V_1| - |V_2|| \leq 1 \). The weight \( w(e) = 1 \) for all \( e \) running between \( V_1 \) and \( V_2 \), \( w(e) = 2 \) otherwise. Clearly every minimum spanning tree only uses crossing edges (having weight 1). However, the proposed algorithm creates a tree containing subtrees in \( V_1 \) and \( V_2 \), whose edges have weight 2.

1. (a) The cycle index polynomial is

\[
P_{D_{10}}(z_1, z_2, z_5, z_{10}) = \frac{1}{20}(z_1^{10} + 4z_1^5 + 4z_2^2 + 6z_5^2 + 5z_4^2z_2^2).
\]

Thus, \( P_{D_{10}}(3, 3, 3, 3) = (3^{10} + 4 \cdot 3^5 + 4 \cdot 3^2 + 6 \cdot 3^5 + 5 \cdot 3^2 \cdot 3^4)/20 = 3210 \).

(b) Substitute \( (R^2 + B^2 + G^2) \) for \( z_i \) in \( P_{D_{10}} \) to obtain

\[
(R + B + G)^{10} + 4(R^{10} + B^{10} + G^{10}) + 4(R^5 + B^5 + G^5)^2 + 6(R^2 + B^2 + G^2)^5 + 5(R + B + G)^2(R^2 + B^2 + G^2)^4)/20.
\]

The coefficient of \( R^4B^4G^2 \) in this polynomial is

\[
\frac{1}{20}((\binom{4}{2} + 3\binom{4}{2} + 5(\binom{4}{2} + \binom{4}{2} + \binom{4}{2} + \binom{4}{2})) = 174.
\]

**Problem 2.** Suppose we have \( n \) employees in a company, and wish to form committees of these employees. Suppose we are not allowed to have a committee all of whose members are also in another committee. Determine the maximum number of committees we can have. Give an example to show how to achieve this number of committees. (For example, if \( n = 3 \), we could choose committees \( \{a, b\}, \{a, c\}, \{b, c\} \) or we could choose committees \( \{a\}, \{b\}, \{c\} \). In fact, it is not hard to see that the maximum number of committees one can choose is 3)

**Sol:** View the employees as the elements from \( [n] = \{1, \ldots, n\} \), and committees as subsets of \( [n] \) so that no two subsets satisfy \( A \subset B \). Then we are asking for the maximum size of an antichain in the Boolean lattice, and by Sperner's theorem, this maximum is \( \binom{n}{\lfloor n/2 \rfloor} \). Equality holds for the middle level of the Boolean lattice when \( n \) is even, and either of the two middle levels when \( n \) is odd.
1. Let $T$ be a spanning tree of $G$. We know that $T$ has at least two leaves $u, v$. Either $G \setminus \{u\}$ or $G \setminus \{v\}$ is connected. Hence $u$ and $v$ are not cut-vertices of $G$.

2. (1) Hall’s Theorem: Given a bipartite graph $G$ with partition sets $X$ and $Y$. $G$ has a matching covering all vertices in $X$ if and only if $|N(S)| \geq |S|$ for all $S \subseteq X$, where $N(S)$ is the union of neighbors of $x \in S$.

(2) We only need to show that Hall’s condition, $|N(S)| \geq |S|$ for all $S \subseteq X$, holds in $G$. Let $d(y, S)$ denote the degree of a vertex $y$ in a set $S$, and $d(y)$ denotes the degree of $y$. For any $S \subseteq X$, we have

$$|S|k = \sum_{x \in S} d(x) = \sum_{y \in N(S)} d(y, S) \leq \sum_{y \in N(S)} k = |N(S)|k,$$

which implies that $|S| \leq |N(S)|$.

Question 7
Is the ternary code with the following parity-check matrix perfect? Give reasons.

$$\begin{pmatrix}
1 & 0 & 2 & 2 \\
0 & 1 & 1 & 2
\end{pmatrix}$$

Solution. Yes. $9[(4) + (2)2] = 3^4$.

1. a) Alice computes $\phi(n) = (p-1)(q-1) = 60$; note she chose $e$ relatively prime to $\phi(n)$. She then computes $d = e^{-1} \pmod{\phi(n)}$. This computation may be done by Euclid’s extended algorithm, which performs only $O(\log(n))$ arithmetic operations, and is feasible even for 200-digit integers.

\[
\begin{align*}
60 &= 1 \cdot 53 + 7 \\
53 &= 7 \cdot 7 + 4 \\
7 &= 1 \cdot 4 + 3 \\
4 &= 1 \cdot 3 + 1 \\
3 &= 3 \cdot 1
\end{align*}
\]

So $d = 53^{-1} \pmod{60} = 17$. Alice’s secret key is $d$. She may discard $p$, $q$, and $\phi(n)$.

b) Alice decrypts 3 as $3^d = 3^{17} \pmod{77}$. She computes $3^{17} \pmod{77}$ by fast exponentiation, which performs only $O(\log(n))$ arithmetic operations.

\[
\begin{align*}
3^2 &= 9 \pmod{77} \\
3^4 &= 9^2 = 81 = 4 \pmod{77} \\
3^8 &= 4^2 = 16 \pmod{77} \\
3^{16} &= 16^2 = 256 = 25 \pmod{77} \\
3^{17} &= 3^{16} \cdot 3 = 75 \pmod{77}
\end{align*}
\]

Bob’s message was 75.

c) Eve knows $n$, but not $p$ and $q$. If $p$ and $q$ have 200 digits (and have been chosen with some care), there is no known method for factoring $n$ in any reasonable time. Without factoring $n$, she cannot compute $\phi(n)$, and cannot compute $d$ given $e$. 
1. Let $M = (Q, \delta, q_0, F)$ be a DFA such that $L = L(M)$. Construct $M' = (Q, \delta, q_0, F')$, where

$$F' = \{ q \in Q \mid \text{some string } s \text{ takes } q \text{ in } M \text{ to a state in } F \}.$$ Then $L(M') = \text{Pref}(L)$.

2. The following is a context-free grammar for the language:

$$
S \rightarrow Acc \\
A \rightarrow aAc \mid B \\
B \rightarrow Bb \mid \varepsilon.
$$
CUT THIS OUT:

1. NA#1

Newton's $f(a) = -0.6851$; $f(b) = 0.3304$;

$k = 1; 2; 3; 4; 5$

$kfe = 3; 5; 7; 9; 11$

$xk = 4.000; 3.633; 3.645; 3.645; 3.645$

$fk = 3.304e-01; -1.155e-02; 5.740e-05; 5.740e-05; 5.740e-05$

$dfk = 0.8997; 0.9687; 0.9659; 0.9659; 0.9659$

$xk+1 = 3.633; 3.645; 3.645; 3.645; 3.645$

$dxk = 3.670e-01; 1.200e-02; 0.000e+00; 0.000e+00; 0.000e+00$

$xzero = 3.645$

2. NA#2

$am = -6.657e+00 -1.066e+01 7.542e+00 | 4.689e+01 | 1.066e+01 | 6.245e-01$

$am = 7.745e+00 3.865e+00 4.062e+00 | 8.058e+01 | 1.745e+00 | 1.000e+00$

$am = 5.643e-01 7.583e+00 -2.704e+00 | 5.756e+01 | 3.758e+00 | 7.442e-02$

FGE $k = 1$

$am = -8.595e-01 -7.338e+00 1.103e+01 | 1.161e+02 | 2.103e+01 | 6.653e+01$

$am = 7.745e+00 3.865e+00 4.062e+00 | 8.058e+01 | 1.745e+00 | 1.000e+00$

$am = 7.286e-02 7.301e+00 -3.000e+00 | 5.169e+01 | 3.730e+00 | 1.000e+00$

FGE $k = 2$

$am = -8.595e-01 -1.005e+00 8.015e+00 | 1.680e+02 | 2.103e+01 | 6.653e-01$

$am = 7.745e+00 3.865e+00 4.062e+00 | 8.058e+01 | 1.745e+00 | 1.000e+00$

$am = 7.286e-02 7.301e+00 -3.000e+00 | 5.169e+01 | 1.730e+00 | 1.000e+00$

BS $k = 3; -1; 1$

$x = -8.419e+00$

$1.569e+01$

$2.096e+01$

Relative Residual;

$r = 1.980e-02$

$3.785e-03$

$9.412e-03$

$rnorm = 1.980e-02; bnorm = 8.058e+01; relres = 2.457e-04$