RYERSON UNIVERSITY

DEPARTMENT
OF
MATHEMATICS

MTH 210 **Final Exam** **April 25, 2007**

Total marks: 70 **Time allowed: 3 hrs.**

NAME (Print): _____ **STUDENT #:** _____

Circle your Lab Section:

011	021	031
ENG 102	ENG 105	LG 06

Instructions:

- Verify that your paper contains 9 questions on 8 pages.
- You are allowed an $8\frac{1}{2} \times 11$ formula sheet written on both sides.
- No other aids allowed. Electronic devices such as calculators, cellphones and ipods must be turned off and kept inaccessible during the test.
- Please keep your Ryerson photo ID card displayed on your desk during the exam.
- In every question show all your work. The correct answer alone may be worth nothing.
- Delete all irrelevant and incorrect work because marks may be deducted for work which is misleading, irrelevant or incorrect, even if steps for a correct solution are also shown.
- Please write only in this booklet. Use of scrap paper or additional enclosures is not allowed. If you need more space continue on the back of the page, directing marker where the answer continues with a bold sign.

---

1. Consider the following recursively defined language L over the alphabet $\Sigma = \{a, b\}$:

   (a) $b \in L$.

   (b) Given a string $s \in L$, the following are also in L:

      i. $as \in L$.

      ii. $bs \in L$.

      (Here as means the concatenation of a with s etc.)

   (c) Nothing else is in L, other than those obtained from repeated applications of the above rules.

8 Mk

Use structural induction to show that every string in L ends in an b.

Be sure to lay out your proof clearly and correctly.

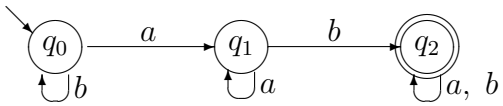
4 Mk 2. Find all trees with 5 vertices, up to isomorphism.

3. Find x when $4x + 1 \equiv 3 \pmod 7$. Your answer should be an integer between 0 and 6. (Be sure to show all your working.)

6 Mk

4. For the following FSA M, find the language accepted by M.
   (Give your answer as both a regular expression and in English.)

[4 Mk]



5. Let L be the regular language over $\{0, 1\}$ consisting of all strings with an odd number of 1's.

[4 Mk] (a) Design an FSA which recognizes L. (Your FSA should have at most 4 states.)

[4 Mk] (b) Find a regular expression for L.

8 Mk 6. Use the Pumping Lemma to show that $L = \{a^n b^m a^{nm} \mid m, n \in \mathbb{N}\}$ is not regular.

7. Consider the classes of languages:

$$\mathcal{L} = \{ \text{ Decidable, Regular, Recognizable, Finite, All Languages } \}.$$

(a) Draw a Venn diagram showing the containment relationships between the classes of languages in $\mathcal{L}$.

4 Mk

(b) Where possible, for each class in $\mathcal{L}$ give an example of a language which is in the class, but not in the one below.

4 Mk

(c) For each language class in $\mathcal{L}$ give the type of machine associated with that language class, where such a machine type exists.

4 Mk

8. Suppose that we are using the RSA cipher with primes $p = 5$ and $q = 7$.

   (a) Given that our encryption key is $e = 19$, find the corresponding decryption key d. (Be sure to show all your working.)

6 Mk

   (b) Using the key pair from part 8a, if the ciphertext message $C = 7$ is received write down the expression which would have to be evaluated to obtain the corresponding plaintext x. (Do not evaluate the expression, just write down what you would have to find – One line answer.)

2 Mk

   (c) Suppose that we are encrypting the plaintext message $x = 3$, with the encryption key $e = 5$. Find the corresponding ciphertext C. (You must use the fastpower algorithm.)

6 Mk

9. At a bank the combination to the safe is shared amongst three employees, Albert, Betty and Charlie. Each is given a digit (0 - 9) of the combination, and the three must each enter their digit in order to open the safe.

6 Mk

Albert is completely trusted and may have any digit, but Betty and Charlie do not have the same digit, to avoid collusion.

(a) How many combinations are there in total?

(b) What is the probability that a random choice of three digits gets the combination?

(c) Betty has the digit 4. Given this information, how many combinations are there?

(d) What is the probability that Betty, guessing the rest of the combination at random, gets the right combination?

(e) What is the probability that Albert, guessing the rest of the combination at random, gets the right combination?

(f) Was this really a good scheme, given that Albert is trusted but Betty and Charlie are not?