University of Toronto
Scarborough Campus
December 14, 1999

CSC B38F Final Examination

Aids allowed: One 8.5×11 handwritten, non-photocopied 'cheat sheet'

Duration: Three hours

- There should be 11 pages in this exam booklet, including this cover page.
- Answer all questions.
- Put all answers in this booklet, in the spaces provided.
- For rough work, use the backs of the pages; ***these will not be marked***.
- Good luck!

Name ______________________________

Student Number ______________________________

Problem	Marks Rec'ved	Marks Worth
1.		10
2.		25
3.		20
4.		20
5.		20
6.		15
7.		20
8.		20
TOTAL		150

QUESTION 1. (10 marks)

Let $f : \mathbb{N} \to \mathbb{N}$ be defined by

$$f(n) = \begin{cases} 3, & \text{if } n = 0 \\ 6, & \text{if } n = 1 \\ 5f(n-1) - 6f(n-2) + 2, & \text{if } n > 1 \end{cases}$$

Prove that $f(n) = 1 + 2^n + 3^n$ for all $n \geq 0$.

Proof:

QUESTION 2. (25 marks)

Recall that if x and m are nonnegative integers such that $m \neq 0$, the remainder of the division of x by m is the (unique) integer r such that $0 \leq r < m$ and, for some (unique) integer q (the quotient of the division), $x = qm + r$.

The algorithm $\textsc{Mod}(x, m)$ below returns the remainder of the division of x by m. More precisely, it satisfies the following precondition/postcondition pair:

Precondition: $x, m \in \mathbb{N}$ and $m \neq 0$.

Postcondition: The integer r returned by the algorithm is such that (a) $0 \leq r < m$ and (b) there is some $q \in \mathbb{N}$ such that $x = qm + r$.

```
MOD(x, m)
r := x
while r ≥ m do
    r := r − m
end while
return r
```

Prove that Mod is correct with respect to the given specification. Make sure you prove both partial correctness and termination.

Proof:

[more space, if needed, available on the next page]

[this space was intentionally left blank]

QUESTION 3. (20 marks)

Consider the following recurrence defining a function $f : \mathbb{N} \to \mathbb{N}$:

$$f(n) = \begin{cases} 4, & \text{if } n = 0 \\ 7f(\lfloor \frac{n}{3} \rfloor) + 5n^2, & \text{if } n > 0 \end{cases}$$

Prove that $f(n) \in O(n^2)$ by exhibiting explicit constants c and n_0, and proving by induction that $f(n) \leq c \cdot n^2$ for every integer $n \geq n_0$.

Do ***not*** use the general theorem about divide and conquer recurrences.

QUESTION 4. (20 marks)

Consider the propositional formula $(\neg x \rightarrow (y \wedge z)) \wedge (\neg y \rightarrow (x \wedge z))$, where x, y, z are propositional variables.

a. (5 marks) Give the truth table of the above formula.

b. (5 marks) Using part (a), write a DNF formula that is logically equivalent to the given formula.

c. (5 marks) Using part (a), write a CNF formula that is logically equivalent to the given formula.

d. (5 marks) Using only substitution of logically equivalent subformulas (and in particular without using truth tables), derive a CNF formula that is logically equivalent to the given formula. Show the steps through which you obtained your formula.

QUESTION 5. (20 marks)

Consider the first-order language of arithmetic with ternary predicate symbols S and P, binary predicate symbols L and $\approx$, and constant symbols $\boldsymbol{0}$ and $\boldsymbol{1}$. Let $\mathcal{N}$ and $\mathcal{Z}$ be structures for this language, with domains $\mathbb{N}$ and $\mathbb{Z}$, respectively, and the standard meaning for the predicate and constant symbols. More formally:

$$
\begin{array}{ll}
S^{\mathcal{N}} = \{(a,b,c) \in \mathbb{N}^3 : a+b=c\} & S^{\mathcal{Z}} = \{(a,b,c) \in \mathbb{Z}^3 : a+b=c\} \\
P^{\mathcal{N}} = \{(a,b,c) \in \mathbb{N}^3 : a \cdot b=c\} & P^{\mathcal{Z}} = \{(a,b,c) \in \mathbb{Z}^3 : a \cdot b=c\} \\
L^{\mathcal{N}} = \{(a,b) \in \mathbb{N}^2 : a<b\} & L^{\mathcal{Z}} = \{(a,b) \in \mathbb{Z}^2 : a<b\} \\
\approx^{\mathcal{N}} = \{(a,b) \in \mathbb{N}^2 : a=b\} & \approx^{\mathcal{Z}} = \{(a,b) \in \mathbb{Z}^2 : a=b\} \\
\boldsymbol{0}^{\mathcal{N}} = 0 & \boldsymbol{0}^{\mathcal{Z}} = 0 \\
\boldsymbol{1}^{\mathcal{N}} = 1 & \boldsymbol{1}^{\mathcal{Z}} = 1
\end{array}
$$

PART I.

For each of the sentences below, state whether it is true or false in each of $\mathcal{N}$ and $\mathcal{Z}$. Justify your answer.

a. (4 marks) $\forall x\, \exists y\, S(x,y,\boldsymbol{0})$

Answer:

b. (4 marks) $\exists x\, \forall y\, S(x,y,\boldsymbol{0})$

Answer:

c. (4 marks) $\exists x\, \forall y\, S(x,y,y)$

Answer:

[continued on the next page]

PART II.

As we have seen, the formula $Prime(x)$ below expresses the predicate "x is prime" in $\mathcal{N}$:

$$Prime(x): \qquad L(\mathbf{1}, x) \wedge \forall y \forall z \Big(P(y, z, x) \rightarrow (\approx(y, \mathbf{1}) \vee \approx(z, \mathbf{1}))\Big)$$

This means that an interpretation $(\mathcal{N}, \sigma)$ satisfies $Prime(x)$ if any only if $\sigma(x)$ is a prime number.

d. (8 marks) Recently, Professor John Friedlander of the Mathematics Department at U of T together with Professor Henryk Iwaniec of Rutgers University in New Jersey, proved that there are infinitely many primes of the form $y^2 + z^4$, where y and z are integers. Write a first-order formula in the language of arithmetic that expresses this fact in $\mathcal{N}$. Your formula may contain the predicate $Prime(x)$, as a shorthand for the formula given above.

Formula:

QUESTION 6. (15 marks)

Consider a relational database whose schema consists of the following relations. (This is the same database schema that you saw in a homework assignment.)

- *Student*(s, n, a) — a tuple (s, n, a) belongs to this relation if the student whose SIN is s has name n and address a. We assume that the SIN uniquely identifies a student.
- *Course*(c, n) — a tuple (c, n) belongs to this relation if there is a course whose code is c (e.g., CSCB38) and whose name is n (e.g., Discrete Mathematics).
- *Takes*(s, c, y, m) — a tuple (s, c, y, m) belongs to this relation if the student whose SIN is s took (or is now taking) course c in year y and received a mark of m. We assume that if a student is presently taking the course but has not completed it yet, the mark m has value I (for "incomplete").
- *Teaches*(n, c, y) — a tuple (n, c, y) belongs to this relation if the professor whose name is n taught (or is now teaching) course c in year y. We assume that each professor is uniquely identified by her/his name, and that each course is offered only once in each year.

Write formulas to express the following queries:

a. (5 marks) Find the names and addresses of all students who took CSCB38 in 1998.

Answer:

b. (5 marks) Find the names of all students who received an A in some course taught by MacLean.

Answer:

c. (5 marks) Find the name of every student who has received an A in every course that she/he has completed (i.e., every course that the student has taken except those that she/he is presently taking).

Answer:

QUESTION 7. (20 marks)

For each of the following statements, indicate whether it is true or false, and justify your answer. **(No credit will be given without correct justification!)**

a. The string 10011 belongs to the language denoted by the regular expression $((00)^*1)^*$.

Answer (true or false):

Justification:

b. $(10 + 01)^* \equiv (10)^* + (01)^*$.

Answer (true or false):

Justification:

c. If there is a NFSA with n states that accepts L, then there is a DFSA with at most 2^n states that accepts L.

Answer (true or false):

Justification:

d. The language $L = \{0^i 1^j : i, j \in \mathbb{N} \text{ and } i \neq j\}$ is regular.

Answer (true or false):

Justification:

QUESTION 8. (20 marks)

Let L be the set of nonempty strings over $\{0, 1\}$ such that the first and last symbol of x are different.

a. (8 marks) Draw the diagram of a DFSA that accepts L.

b. (7 marks) Briefly explain why your DFSA is correct by providing appropriate state invariants. (You **need not** prove that the state invariant you provided is a correct one — but it should be!)

c. (5 marks) Give a regular expression that denotes L. (You **need not** prove that your expression is correct — but it should be!)

THE END