## CS202 Final Exam

December 20th, 2007

Write your answers in the blue book(s). Justify your answers. Work alone. Do not use any notes or books.

There are six problems on this exam, each worth 20 points, for a total of 120 points. You have approximately three hours to complete this exam.

## 1 A coin-flipping problem (20 points)

A particularly thick and lopsided coin comes up heads with probability $p_{H}$, tails with probability $p_{T}$, and lands on its side with probability $p_{S}=1-$ $\left(p_{H}+p_{T}\right)$. Suppose you flip the coin repeatedly. What is the probability that it comes up heads twice in a row at least once before the first time it comes up tails?

## 2 An ordered group (20 points)

Let $G$ be a group and $\leq$ a partial order on the elements of $G$ such that for all $x, y$ in $G, x \leq x y$. How many elements does $G$ have?

## 3 Weighty vectors (20 points)

Let the weight $w(x)$ of an $n \times 1$ column vector $x$ be the number of nonzero elements of $x$. Call an $n \times n$ matrix $A$ near-diagonal if it has at most one nonzero off-diagonal element; i.e., if there is at most one pair of indices $i, j$ such that $i \neq j$ and $A_{i j} \neq 0$.

Given $n$, what is the smallest value $k$ such that there exists an $n \times 1$ column vector $x$ with $w(x)=1$ and a sequence of $k n \times n$ near-diagonal matrices $A_{1}, A_{2}, \ldots A_{k}$ such that $w\left(A_{1} A_{2} \cdots A_{k} x\right)=n$ ?

## 4 A dialectical problem (20 points)

Let $S$ be a set with $n$ elements. Recall that a relation $R$ is symmetric if $x R y$ implies $y R x$, antisymmetric if $x R y$ and $y R x$ implies $x=y$, reflexive if $x R x$ for all $x$, and irreflexive if $\neg(x R x)$ for all $x$.

1. How many relations on $S$ are symmetric, antisymmetric, and reflexive?
2. How many relations on $S$ are symmetric, antisymmetric, and irreflexive?
3. How many relations on $S$ are symmetric and antisymmetric?

## 5 A predictable pseudorandom generator (20 points)

Suppose you are given a pseudorandom number generator that generates a sequence of values $x_{0}, x_{1}, x_{2}, \ldots$ by the rule $x_{i+1}=\left(a x_{i}+b\right) \bmod p$, where $p$ is a prime and $a, b$, and $x_{0}$ are arbitrary integers in the range $0 \ldots p-1$. Suppose further that you know the value of $p$ but that $a, b$, and $x_{0}$ are secret.

1. Prove that given any three consecutive values $x_{i}, x_{i+1}, x_{i+2}$, it is possible to compute both $a$ and $b$, provided $x_{i} \neq x_{i+1}$.
2. Prove that given only two consecutive values $x_{i}$ and $x_{i+1}$, it is impossible to determine $a$.

## 6 At the robot factory (20 points)

Each robot built by Rossum's Combinatorial Robots consists of a head and a body, each weighing a non-negative integer number of units. If there are exactly $3^{n}$ different ways to build a robot with total weight $n$, and exactly $2^{n}$ different bodies with weight $n$, exactly how many different heads are there with weight $n$ ?

