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 $p_S = 1 - (p_H + p_T)$. 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?

Solution

Let p be the probability of the event W that the coin comes up heads twice before coming up tails. Consider the following mutually-exclusive events for the first one or two coin-flips:

Event A	$\Pr[A]$	$\Pr[W\|A]$
HH	p_H^2	1
HT	$p_H p_T$	0
HS	$p_H p_S$	p
T	p_T	0
S	p_S	p

Summing over all cases gives

$$p = p_H^2 + p_H p_S p + p_S p,$$

which we can solve for p to get

$$p = \frac{p_H^2}{1 - p_H p_S - p_S} = \frac{p_H^2}{p_H + p_T - p_H p_S} = \frac{p_H^2}{p_T + p_H(p_H + p_T)} = \frac{p_H^2}{p_T + p_H p_T + p_H^2}.$$

(Any of these is an acceptable answer.)

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, $x \leq xy$. How many elements does G have?

Solution

The group G has exactly one element.

First observe that G has at least one element, because it contains an identity element e.

Now let x and y be any two elements of G. We can show $x \leq y$, because $y = x(x^{-1}y)$. Similarly, $y \leq x = y(y^{-1}x)$. But then $x = y$ by antisymmetry. It follows that all elements of G are equal, i.e., that G has at most one element.

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 $A_{ij} \neq 0$.

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 $w(A_1 A_2 \cdots A_k x) = n$?

Solution

Let's look at the effect of multiplying a vector of known weight by just one near-diagonal matrix. We will show: (a) for any near-diagonal A and any x, $w(Ax) \leq w(x)+1$, and (b) for any $n \times 1$ column vector x with $0 < w(x) < n$, there exists a near-diagonal matrix A with $w(Ax) \geq w(x) + 1$.

To prove (a), observe that $(Ax)_i = \sum_{j=1}^{n} A_{ij} x_j$. For $(Ax)_i$ to be nonzero, there must be some index j such that $A_{ij} x_j$ is nonzero. This can occur in two ways: $j = i$, and A_{ii} and x_i are both nonzero, or $j \neq i$, and A_{ij} and x_j are both nonzero. The first case can occur for at most $w(x)$ different values of i (because there are only $w(x)$ nonzero entries x_i). The second can occur for at most one value of i (because there is at most one nonzero entry A_{ij} with $i \neq j$). It follows that Ax has at most $w(x) + 1$ nonzero entries, i.e., that $w(Ax) \leq w(x) + 1$.

To prove (b), choose k and m such that $x_k = 0$ and $x_m \neq 0$, and let A be the matrix with $A_{ii} = 1$ for all i, $A_{km} = 1$, and all other entries equal to zero. Now consider $(Ax)_i$. If $i \neq k$, then $(Ax)_i = \sum_{j=1}^{n} A_{ij} x_j = A_{ii} x_i = x_i$. If $i = k$, then $(Ai)_k = \sum_{j=1}^{n} A_{ij} x_j = A_{kk} x_k + A_{km} x_m = x_m \neq 0$, since we chose k so that $a_k = 0$ and chose m so that $a_m \neq 0$. So $(Ax)_i$ is nonzero if either x_i is nonzero or $i = k$, giving $w(Ax) \geq w(x) + 1$.

Now proceed by induction:

For any k, if $A_1 \dots A_k$ are near-diagonal matrices, then $w(A_1 \cdots A_k x) \leq w(x)+k$. Proof: The base case of $k = 0$ is trivial. For larger k, $w(A_1 \cdots A_k x) = w(A_1(A_2 \cdots A_k x)) \leq w(A_2 \cdots A_k x) + 1 \leq w(x) + (k-1) + 1 = w(x) + k$.

Fix x with $w(x) = 1$. Then for any $k < n$, there exists a sequence of near-diagonal matrices $A_1 \dots A_k$ such that $w(A_1 \cdots A_k x) = k + 1$. Proof: Again the base case of $k = 0$ is trivial. For larger $k < n$, we have from the induction hypothesis that there exists a sequence of $k - 1$ near-diagonal matrices $A_2 \dots A_k$ such that $w(A_2 \dots A_k x) = k < n$. From claim (b) above we then get that there exists a near-diagonal matrix A_1 such that $w(A_1(A_2 \dots A_k x)) = w(A_2 \dots A_k x) + 1 = k + 1$.

Applying both these facts, setting $k = n - 1$ is necessary and sufficient for $w(A_1 \dots A_k x) = n$, and so $k = n - 1$ is the smallest value of k for which this works.

4 A dialectical problem (20 points)

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

Solution

Since in all three cases we are considering symmetric antisymmetric relations, we observe first that if R is such a relation, then xRy implies yRx which in turn implies $x = y$. So any such R can have xRy only if $x = y$.

1. Let R be symmetric, antisymmetric, and reflexive. We have already established that xRy implies $x = y$. Reflexivity says $x = y$ implies xRy, so we have xRy iff $x = y$. Since this fully determines R, there is exactly 1 such relation.

2. Now let R be symmetric, antisymmetric, and irreflexive. For $x \neq y$ we have $\neg(xRy)$ (from symmetry+antisymmetry); but for $x = y$, we again have $\neg(xRy)$ (from irreflexivivity). So R is the empty relation, and again there is exactly 1 such relation.

3. Now for each x there is no constraint on whether xRx holds or not, but we still have $\neg(xRy)$ for $x \neq y$. Since we can choose whether xRx holds independently for each x, we have n binary choices giving 2^n possible relations.

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 $x_{i+1} = (ax_i + b) \bmod p$, 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.

Solution

1. We have two equations in two unknowns:

$$\begin{aligned} ax_i + b &= x_{i+1} \pmod{p} \\ ax_{i+1} + b &= x_{i+2} \pmod{p}. \end{aligned}$$

   Subtracting the second from the first gives

$$a(x_i - x_{i+1}) = x_{i+1} - x_{i+2} \pmod{p}.$$

   If $x_i \neq x_{i+1}$, then we can multiply both sides by $(x_i - x_{i+1})^{-1}$ to get

$$a = (x_{i+1} - x_{i+2})(x_i - x_{i+1})^{-1} \pmod{p}.$$

   Now we have a. To find b, plug our value for a into either equation and solve for b.

2. We will show that for any observed values of x_i and x_{i+1}, there are at least two different values for a that are consistent with our observation; in fact, we'll show the even stronger fact that for *any* value of a, x_i and x_{i+1} are consistent with that choice of a. Proof: Fix a, and let $b = x_{i+1} - ax_i \pmod{p}$. Then $x_{i+1} = ax_i + b \pmod{p}$.

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?

Solution

This is a job for generating functions!

Let $R = \sum 3^n z^n = \frac{1}{1-3z}$ be the generating function for the number of robots of each weight, and let $B = \sum 2^n z^n = \frac{1}{1-2z}$ be the generating function for the number of bodies of each weight. Let $H = \sum h_n z^n$ be the generating function for the number of heads. Then we have $R = BH$, or

$$H = \frac{R}{B} = \frac{1-2z}{1-3z} = \frac{1}{1-3z} - \frac{2z}{1-3z}.$$

So $h_0 = 3^0 = 1$, and for $n > 0$, we have $h_n = 3^n - 2 \cdot 3^{n-1} = (3-2)3^{n-1} = 3^{n-1}$.