15-251 : Great Theoretical Ideas In Computer Science

Fall 2014

Assignment 8

Due: Halloween, **Friday**, October 31, 2014 11:59 PM

Name: _____

Andrew ID: _____

Question:	1	2	3	4	Total
Points:	25	20	25	25	95
Score:					

0. Warmup

(a) Given the following transition matrix for a Markov process with three states 1,2 and 3.

```
    1/3 1/3 1/4
M = 1/2 0   1/2
    1/3 1/3 1/3
```

i. What is $Pr[X_1 = 3 | X_0 = 3]$?

ii. What is $Pr[X_2 = 1 | X_0 = 3]$?

(b) Given the following transition matrix for a Markov process with two states

```
    (1-p) p
M =  q   (1-q)
```

Compute the invariant (stationary) distribution for this Markov process.

(c) Suppose Alice wants to send Bob 5 numbers between 0 and 6 inclusive and recover from the loss of any single number.

i. What's the smallest prime field Alice can use?

ii. Suppose Alice sends $(2, 3, 5, 1, 6)$. What is the maximum degree for which a unique polynomial $P(x)$ fits the points $(1, 2), (2, 3), (3, 5), (4, 1), (5, 6))$? (Notice that this differs from the encoding used in lecture, where our message is the coefficients instead of the values.)

iii. What are the coefficients of $P(x)$?

iv. What is the minimum number of extra points Alice must send Bob so that he can correctly reconstruct her message?

v. What is $P(6)$?

vi. Alice sends $(2, 3, 5, 1, 6, 6)$, but Bob receives $(2, X, 5, 1, 6, 1)$. Can Bob recover the lost 2nd packet?

vii. What size is the system of linear equations Bob must solve to recover the packet? What are the equations?

viii. Solve this system using Gaussian elimination.

ix. Could Bob have still decoded Alice's message if the second and sixth points were both missing?

(d) Suppose Alice wants to send Bob 3 numbers between 0 and 6 inclusive and she wants to guard against 1 corrupted packet.

i. What's the smallest prime field Alice can use?

ii. Suppose Alice wants to send Bob $m = ((1, m_1), (2, m_2), (3, m_3))$. what is the maximum degree for which a unique polynomial fits these points?

iii. What is the minimum number of extra points Alice must send Bob so that he can correctly reconstruct her message m?

iv. Bob receive a message $r = (3, 3, 3, 2, 0)$. In order to check whether the message is corrupted, Bob needs to solve $N(x) = r_i E(x)$, where $N(x) = P(x)E(x)$, $P(x)$ is the original polynomial used to send the message, and $E(x)$ is the error-locator polynomial from the Berlekamp-Welch algorithm. What are the degrees of $N(x)$ and $E(x)$?

v. What is the solution to the corresponding system of linear equations:

$$a_3 + a_2 + a_1 + a_0 = 3 + 3b_0$$

$$a_3 + 4a_2 + 2a_1 + a_0 = 6 + 3b_0$$

$$6a_3 + 2a_2 + 3a_1 + a_0 = 2 + 3b_0$$

$$a_3 + 2a_2 + 4a_1 + a_0 = 1 + 2b_0$$

$$6a_3 + 4a_2 + 5a_1 + a_0 = 0$$

vi. What is the original polynomial $P(x) = ax^2 + bx + c$?

vii. Which packet is corrupted, and what is the original value?

1. Gambling

Victor starts out with zero dollars. Every day he gains a dollar with probability p, stays put with probability s, or loses all his money (goes broke) with probability b, where $p + s + b = 1$. Victor plays the game forever. Model this process, using the infinite Markov chain.

(5) (a) Write the transition matrix for this Markov process (for the first three states).

Solution:

(5) (b) Write the system of stationary equations for this Markov process. It's sufficient to show only the first three equations. Hint: See the slide #4 in the lecture notes.

Solution:

(10) (c) Compute the invariant (stationary) distribution for this Markov process.

Solution:

(5) (d) What is Victor's long-run expected money in the particular case $s = 0$?

Solution:

2. Playing Random Chess

In chess, a rook can move either horizontally within its row (left or right) or vertically within its column (up or down) any number of squares. In an 8×8 chess board, imagine a rook that starts at the lower left corner of a chess board. At each move, a bored TA decides to move the rook to a random legal location (assume that the move cannot involve staying still).

(8) (a) Define states and write the transition matrix for this Markov process.

Solution:

(12) (b) Let T denote the time until the rook first lands in the upper right corner of the board. Compute $E[T]$.

Solution:

3. Protect the code

Imagine that you are the CEO of a promising new start-up, and the launch of an exciting new web product is impending. For some reason, presumably due to your affection to 15-251, releasing the product requires a secret code $s \in \{0, 1, 2, \ldots, 250\}$ that only you as CEO know. Unfortunately, due to things beyond your control, you are forced to take a vacation around the planned launch date.

(10) (a) You have a trusted group of 5 employees in senior management, but you are not willing to share the code with all of them lest one of them misuse it when the site is still premature. So you come up with a scheme to break the secret into pieces $m_1, m_2, \ldots, m_5$ (with m_i revealed privately to manager i) in the following controlled way:

- If a majority (i.e., at least three) of the senior managers agree on the release, then they can put their pieces together to correctly determine the code s and release the product.
- On the other hand, if only two managers agree on the release and share their pieces, they will have no idea about the secret code s, in the sense that every possible value for s in $\{0, 1, 2, \ldots, 250\}$ will be consistent with their knowledge. (We assume that attempting a release with an incorrect code will be devastating so no one will attempt that.)

What was your scheme to achieve these goals?

Solution:

(15) (b) Just before you set off on vacation, you change your mind and decide that you should also involve a group of 7 distinguished engineers in this key decision. So now you would like a scheme to break your code into five pieces $m_1, s_2, \ldots, m_5$ for the managers and seven pieces $e_1, e_2, \ldots, e_7$ for the engineers to ensure the following:

- If a majority of managers *and* a majority of engineers agree on the release, then they can put their pieces together to correctly determine the code s and release the product.
- In all other scenarios, namely if at most 2 managers favor the release or at most 3 engineers favor the release, then pooling the pieces of everyone favoring the release gives no information about s.

What's your new scheme to achieve these goals?

Solution:

4. What color is your hat?

Let $r \geq 3$ be a positive integer, and $n = 2^r - 1$. Consider the Hamming code $C \subseteq \{0,1\}^n$ defined in class

$$C = \{c \in \{0,1\}^n \mid Hc = 0\}$$

where H is $r \times (2^r - 1)$ matrix whose ith column, $i = 1, 2, \ldots, 2^r - 1$, is the r-bit binary representation of i in binary, and the matrix-vector product Hc (where we think of c as a column vector) is computed modulo 2. The strings in C are called the *Hamming codewords*.

(10) (a) Let $z \in \{0,1\}^n \setminus C$. Prove that there is *exactly one codeword* of C differing from z in a single bit position. (For instance, for the case $r = 3$ and $z = (0\ 1\ 1\ 0\ 1\ 0\ 1)$, the codeword $(0\ 1\ 0\ 0\ 1\ 0\ 1)$ is the unique one that differs from z in one bit, namely the 3rd bit.)

Solution:

(15) (b) Hamming codes are useful not only for error-correction, but also for puzzles/games.

Suppose 31 players enter a room and a red or blue hat is placed on each person's head. The color of each hat is determined by a coin toss, with the outcome of one coin toss having no effect on the others. Each person can see the other players' hats but not his/her own.

No communication of any sort is allowed during the game, except for an initial strategy session before the game begins. Once they have had a chance to look at the other hats, the players must *simultaneously* guess the color of their own hats or abstain from guessing. The group wins the game if (i) at least one player guesses correctly, and (ii) no players guess incorrectly.

One obvious strategy for the players, for instance, would be for one player to always guess "red" while the other players pass. This would give the group a 50 percent chance of winning the game. Can you use Hamming codes to devise a strategy for the group that achieves a higher probability of winning (probability being taken over the initial random assignment of hat colors)?

(While you don't have to prove the optimality of your answer, for full credit your strategy must achieve the highest possible probability of winning.)

Solution: