CMSC 858S: Algorithms in Networking

Fall 2004

Homework Assignment #2 **(will be graded)**

Due date: Beginning of class on November 9, 2004

Note: As with all homework assignments for this class, this needs to be done along with your group-mates. Please submit one final, polished set of answers for your group, and do not include unnecessary material. (For instance, don't include your preliminary work/calculations/intuition that led to the final answer.) Partial credit will be given where appropriate: if you think you have some ideas that deserve partial credit, please *itemize them concisely*, so that the grading process can be accurate.

1. Consider a "jackpot" server which tries to choose one among n competing players as the lucky winner for a Million dollar award. Let S be the set of players who are currently competing in the jackpot. The server expects all the n players to comply with rules of the game which are defined as follows:

- The game proceeds in a round-by-round fashion.
- In the beginning of the first round, the server initializes the current set of competing players A to S.
- The server executes the following procedure in each round of the game. Each player in A is requested to send a random bit to the server. Let A_0 and A_1 be the set of players who sent 0 and 1 to the server respectively in the current round; this "each player sending a random bit" is repeated until both A_0 and A_1 are nonempty. If $A_0 \leq |A|/2$, then $A \leftarrow A_0$, else $A \leftarrow A_1$: i.e., if A_1 is strictly smaller in size than A_0, then the set of players in A_1 qualify for the next round; otherwise the set of players in A_0 qualify for the next round. Notice that this diminishes the number of players left in the game by at least half at the end of each round.
- The game terminates when we have only one player left at the end of some round; such a player is declared the winner.

The main difficulty in the above game is that some players can be "bad": they can cheat by colluding among themselves, oberving the bits sent by other players, sending their bits which are not chosen uniformly at random, etc. Let k be a power of two. Assume there are k good players (who do not cheat) and let $n = 2k - 1$. Show that there is a constant $c > 0$ such that for all large enough k, the probability that the winner of this game is a good player, is at least $k^{-c \log k}$.

Hint: Recall from Stirling's approximation that for any i, $\binom{2i}{i}$ is roughly equal to $\frac{2^{2i}}{\sqrt{\pi i}}$.

2. Suppose there are exactly two good players and one bad player. The jackpot rules are now modified as follows so that the server can choose a winner in a single round (of course, the two good players follow these modified rules strictly, while the bad player may not). Let the players be P_0, P_1, and P_2, and let $p \in [0, 1]$. The protocol is as follows. Player P_0 sends 0 with probability $1 - p$, and 1 with probability p; similarly for P_1. Player P_2 does not send anything. If player P_0 sent 0, then player P_1 is winner. If players P_0 and P_1 sent 1, then player P_2 is the winner. If player P_0 sent 1 and P_1 sent 0, then player P_0 is the winner. What should the value of p be, so that the probability of a good player being the winner is maximized? Remember that we know there is exactly one bad player, but we don't know who it is. Thus, we want as

large a value r as possible, so that whether the bad player is P_0, P_1 or P_2, the probability of getting a good winner is at least r.

3. Suppose we have a sequence $X_1, X_2, \ldots, X_n$ of random variables. For any i and any given sequence $(a_1, a_2, \ldots, a_i)$, let $A_i(a_1, a_2, \ldots, a_i)$ denote the event

$$(X_1 = a_1) \wedge (X_2 = a_2) \wedge \cdots \wedge (X_i = a_i),$$

where the "$\wedge$" denotes an AND as usual. Call the sequence $(a_1, a_2, \ldots, a_i)$ "admissible" if $\Pr[A_i(a_1, a_2, \ldots, a_i)]$ is nonzero.

Recall that the sequence $X_1, X_2, \ldots, X_n$ is a Martingale if the following holds for all $i \leq n-1$ and for all admissible $(a_1, a_2, \ldots, a_i)$:

$$\mathbf{E}[X_{i+1} \mid A_i(a_1, a_2, \ldots, a_i)] = a_i.$$

Give an example of two random variables X_1 and X_2 where (X_1, X_2) is a Martingale, but (X_2, X_1) is not.