This homework is due in class May 1, 2003

Homework 10

1. Consider the following distribution over $\{0,1\}^4$. We pick at random two independent and unbiased bits b_1, b_2. Then we set $b_3 = b_1 \oplus b_2$. Finally, if $b_3 = 0$ we set $b_4 = 0$, otherwise we set b_4 to the value of a fresh unbiased random bit. Finally, we output (b_1, b_2, b_3, b_4).

   Compute the entropy of this distribution.

2. Consider the Byzantine agreement algorithm seen in class and in Section 12.6 of Motwani-Raghavan. In the protocol, at every step, all parties receive a fresh random coin. The random coin of step i is not known at step $i-1$.

   Consider now a new model in which all parties know in advance all the random coins. Show that if initially, half of the honest parties has input 0 and half has input 1, then the faulty parties can prevent the honest parties from ever reaching agreement.

3. The analysis in class and in the book shows that if there are fewer than $n/8$ faulty parties then agreement is reached in an expected constant number of rounds. Improve the analysis, possibly by changing the values L, G, H so that a larger fraction of faulty parties can be tolerated.

   [Note: you should be able to tolerate up to $n/4$ faulty parties. Any solution achieving αn with $\alpha > 1/8$ receives full credit.]