ECE 559BH Distributed Network Algorithms **SPRING 2006**
PROBLEM SET 4 **Due Tuesday, March 28**

Byzantine agreement problem, LT codes

Reading: See website.

Problems to be handed in:

1. Byzantine agreement (S. Yang)
The expected number of rounds for the randomized algorithm ByzGen to reach agreement is bounded by a constant (three or four, depending on definition) as long as $t < n/8$, but the algorithm uses common randomness–all nodes see the same coin flip in each round. Specify a variation of ByzGen which uses private, but not common, randomness, and reaches agreement in a constant number of rounds if $t \leq \sqrt{n}$. (Hint: What if each nodes flips a fair coin, and reports the result to all neighbors?)

2. Bounding a martingale (can be used for a minor variation of a part of Luby's proof)
Let $\boldsymbol{\mathcal{F}} = (\mathcal{F}_t : t \in \mathbb{Z}_+)$ be a filtration. Suppose X_0 is an integrable, $\mathcal{F}_0$ measurable random variable, $m = (m_t : t \in \mathbb{Z}_+)$ is an adapted process with values in the positive integers, and for each $t \geq 0$, V_t is an $\mathcal{F}_{t+1}$ measurable random variable such that, given $\mathcal{F}_t$, its conditional distribution is binomial with parameters m_t and $\frac{1}{m_t}$. That is, $(V_t|\mathcal{F}_t) \sim \text{Binom}(m_t, \frac{1}{m_t})$. Let $X_t = X_0 + V_0 + \cdots + V_{t-1} - t$.
(a) Show that X is a martingale relative to $\boldsymbol{\mathcal{F}}$.
(b) Show that if $V \sim \text{Binom}(n, \frac{1}{n})$ for some integer $n \geq 1$, then $E[e^{\alpha(V-1)}] \leq e^{\alpha^2}$ for $|\alpha| \leq 1$.
(c) Show that $E[e^{\alpha(X_t - X_0)}] \leq e^{\alpha^2 t}$ for $|\alpha| \leq 1$.
(d) Using a Chernoff bound, show that for $\lambda \geq 0$, $P\{|X_t - X_0| \geq \lambda\} \leq \begin{cases} 2e^{-\frac{\lambda}{2}} & \text{if } t \leq \frac{\lambda}{2} \\ 2e^{-\frac{\lambda^2}{4t}} & \text{if } t \geq \frac{\lambda}{2} \end{cases}$

3. Reserved packets in the gross ripple
(This problem addresses the output symbols contributed by the term $\tau(k/R)$ in Luby's paper on LT codes.) Suppose that k is large and $R = 3\sqrt{k}\ln(3k/\delta)$ for δ fixed with $0 < \delta < 1$ (that is, R grows somewhat faster than $\sqrt{k}$). Let $t_o = k - R$ and $d = k/R$. Consider a special output symbol of degree d which has been reserved for use after t_o symbols have been decoded, if the special output symbol enters the gross ripple before t_o. (The special output symbol can be forced to leave the ripple early if some other output symbol connected to the same input symbol is decoded.) Let p denote the probability the special output symbol is in the gross ripple after t_o symbols have been decoded, assuming the decoding process successfully decodes at least t_o symbols.
(a) Argue that $p \approx e^{-1}$ based on a Poisson approximation.
(b) Find the exact value of p, and show it converges to e^{-1} as $k \to \infty$. (Hint: $\frac{d}{k} = \frac{o(1)}{d}$.)

4. LT decoding with half degree one and half degree two packets
Consider LT decoding for $k >> 1$ input symbols based on $Poi(k)$ output symbols. Suppose each output symbol is initially degree one or two, with equal probability, independently of all other output symbols.
(a) What is the expected number of input symbols included in one or more output symbols?
(b) What fraction of input symbols are successfully decoded by the LT decoding algorithm (with high probability for large k)?
(c) What fraction of output symbols are not decoded?
(d) What fraction of output symbols are connected to two input symbols which have degree one? (Such output symbols are not decoded. Are these essentially all of the output symbols that are not decoded?)