ECE 559BH Distributed Network Algorithms **SPRING 2006**
PROBLEM SET 5 **Due May 2, 2006**

Network coding, averaging by gossip, on combinatorial auctions, moment method, classical gossip process

Reading: See website.

Problems to be handed in:

0. Midterm
Submit a revised version of your midterm exam.

1. On algebraic gossip for multiple rumor mongering
Suppose the algebraic gossip process of Deb, Médard, and Choute is used, using random linear coding and pull based dissemination. Any message, either original or coded, can be expressed in terms of the k original messages $m_1, \ldots, m_k$ by $\sum_{i=1}^{k} \theta_i m_i$, where $\theta = (\theta_1, \ldots, \theta_k) \in \mathbb{F}_q^k$ is the *code vector* of the message. There are q^k possible code vectors.
(a) Give a reason why the code vectors received during execution of the algorithm are not uniformly distributed over the set of possible code vectors, and why the received code vectors are not independent.
(b) As an approximation, in spite of part (a), suppose a particular node receives m mutually independent code vectors for some $m \geq k$, such that each code vector is uniformly distributed over the set of all q^k possible code vectors. Show that the probability the set of code vectors does not have full rank (i.e. the probability it is not possible to recover the original k messages) is less than or equal to q^{k-m}. (Hint: Given a nonzero vector $u \in \mathbb{F}_q^k$, the set $H_u = \{x \in \mathbb{F}_q^k : x \cdot u = 0\}$ is a $k-1$ dimensional hyperplane of $\mathbb{F}_q^k$. What is the probability that all m received messages are in H_u for fixed u? How many choices of u are there? Use a union bound.)
(c) How large should m be so that the bound (under the approximation of uniformity and independence) on the probability of failure found in part (b) is less than n^{-c}?

2. On minimizing $\lambda_2(W)$
(The paper of Boyd et al on gossip algorithms shows that the rate of convergence for averaging by random gossip is determined by the second largest eigenvalue of the symmetric stochastic matrix W. This suggests using neighbor selection probabilities which minimize the eigenvalue. The paper describes a method based on a projected subgradient method. Here we discuss some basic theory related to that optimization.) Recall that a matrix A is said to be positive semidefinite if it is square and $x^T A x \geq 0$ for all vectors x. Write $A \prec B$ if $B - A$ is positive semidefinite. The second largest eigenvalue of a symmetric stochastic $n \times n$ matrix W is given by $\lambda_2(W) = \min\{s : W - \frac{1}{n}\mathbf{1}\mathbf{1}^T \prec sI\}$. We also have that

$$\lambda_2(W) = \max\left\{u^T(W - \frac{1}{n}\mathbf{1}\mathbf{1}^T)u : ||u|| = 1\right\} \tag{1}$$

and a vector u achieving the maximum in (1) is an eigenvector associated with λ_2. A subgradient of a convex function f over $\mathbb{R}^n$ at a point s is an n-vector $g(s)$ such that $f(\widetilde{s}) \geq (\widetilde{s} - s)^T g(s) + f(s)$ for all $\widetilde{s}$. A subgradient exists, even if f is not differentiable.
(a) Show that if $A \prec B$ and $C \prec D$, then $A + C \prec B + D$.
(b) Show that $\lambda_2(W)$ is a convex function over the space of $n \times n$ symmetric stochastic matrices W.
(c) Show that if W and $\widetilde{W}$ are symmetric stochastic matrices of dimension $n \times n$, and if v is an eigenvector of W corresponding to $\lambda_2(W)$, then $\lambda_2(\widetilde{W}) \geq \lambda_2(w) + \boldsymbol{Tr}(vv^T(\widetilde{W} - W))$. That is, vv^T (viewed as an element of n^2 dimensional space) is a subgradient of the function $\lambda_2(W)$ at W.
(d) Let $f(x)$ be defined on $\mathbb{R}$ by $f(x) = |x|$. Find a subgradient function $g(x)$ for f, and consider a sequence defined by $x_{k+1} = x_k - \nu_k g(x_k)$ for some initial state x_0, such that the constants ν_k are positive, $\lim_{k\to\infty} \nu_k = 0$, and $\sum_k \nu_k = \infty$. Does $\lim_{k\to\infty} x_k = 0$?
(e) Consider again the sequence of part (d), but assume instead that $\nu_k = \epsilon$, where ϵ is a small positive constant. What can you say about $\lim_{n\to\infty} |x_n|$. How does the convergence differ qualitatively from the case that $f(x) = \frac{x^2}{2}$?

3. On computationally feasible mechanisms for combinatorial auctions (X. Zhang)

(a) The Theorem 6.1 in Lehmann et al's paper states that the problem of finding an allocation a that maximizes $\sum_{i=1}^{n} d_i(a)$ is NP-hard. We know that the set packing problem is NP-hard. Show how to reduce set packing problem into the value maximization problem used by the GVA algorithm. (The set packing problem: Given a list G of subsets of some set S, find a maximum cardinality subset of G with disjoint elements.)

(b) The greedy allocation is an approximation to the optimal GVA maximization allocation. Let GRD be the total sum of d_is of a greedy allocation $l = 1$. OPT be the sum of GVA maximization. Show that $OPT/GVA \leq k$ and the bound is tight.

(c) Show that the greedy allocation and critical payment scheme is truthful by directly using the definition of truthful (Definition 3.2).

4. Applying the first and second moment methods

(Exercise 6.13 of Mitzenmacher and Upfal, p. 151) Consider the random graph $G_{n,p}$, with $p = c \ln n/n$.

(a) Show that if $c > 1$ then the probability an isolated vertex exists converges to zero as $n \to \infty$.

(b) Show that if $c < 1$ then the probability an isolated vertex exists converges to one as as $n \to \infty$.

5. The classical gossip process (Lei Ying)

Consider the rumor spreading scenario as in the paper of Frieze and G. R. Grimmett. (a) Using a union bound as in the analysis of the coupon collectors problem, show that if $(1 - \eta)n$ people know the rumor, then after $\frac{(1+\gamma)\log_2 n}{1-\eta}$ rounds, the probability that the rumor is not spread to all people is at most n^{γ}. (Hint: Because of the initial state, in each round, at least $(1-\eta)n$ random calls are made, so that over the specified number of rounds, at least $(1+\gamma)n \log_2 n$ random calls are made. Think of these calls as random coupons, with the type of the coupon being the person called.) (b) (optional) Use the Poission bounding method to show that the constants in part (a) are the best possible.