CSL860: Routing in the presence of faults
I semester, 2008-09

Minor II

September 26, 2008

Due: The exam must be latexed, printed out and handed to me or slipped into my office **by 12PM** on **Thursday, 2nd October 2008**. Note that the 2nd of October is an official holiday, but the building will be open.

Examination notes: Please read these carefully before beginning. For this exam you are **not** allowed to consult the internet or any other source apart from the class notes under any circumstances. You are allowed to consult other students. There will be a 30 percent penalty for it (i.e. your score will be multiplied by 0.7). **Latexing the exam is mandatory**. I will not accept any exam which is not latexed. No extensions of any sort will be given, so if there's a problem meeting the deadline, you must let me know latest by Saturday the 27th of September, 10PM.

Problem 1. We are given a function $\beta : \mathbb{N} \to [0, 1]$. And we are given a family of graphs $\mathcal{G}$ with the property that for all $G \in \mathcal{G}$, $\beta(|G|) \leq \alpha_G$ where $|G|$ denotes the number of nodes in G and α_G is the node expansion of G. In other words the (node) expansion of each graph in the family is at least $\beta(|G|)$. We say that the family $\mathcal{G}$ has *uniform expansion* β if for all subgraphs H of every graph $G \in \mathcal{G}$ it holds that $\alpha_H = O(\beta(|H|)$. Note that we are not talking about the expansion of a subset H *within* G but the expansion of the subgraph itself i.e.

$$\alpha_H = \min_{U \subseteq V(H), |U| \leq |V(H)|/2} \frac{|\Gamma(U)|}{|U|}.$$

Show that for every connected graph of size n with uniform expansion β there is an adversarial selection of $O(\beta(n) \cdot n)$ nodes that makes the graph fall into pieces of size $o(n)$.

Problem 2. In this problem we will talk about the problem of secure communication using shared keys. Let us assume that there is a set of n nodes, $V = \{v_1, v_2, \ldots, v_n\}$ and there is a set of n keys $\{k_1, k_2, \ldots, k_n\}$. We are allowed to make as many copies of the keys as we want. We form a network as follows:

> Distribute copies of the keys to all the nodes. Place an edge between nodes v_i and v_j if there is some key k_l that they both possess.

Q2.1. Suppose each node is given $\lceil fn \rceil$ keys chosen uniformly at random from K for some constant $f < 1$, independent of the choices of keys for all other nodes. Let us call the network formed this way G. Is G connected with high probability (i.e. with probability $> 1 - \frac{1}{n}$) for all constant values of f?

Q2.2. Let us try to say something about the expansion of the network. Recall the definition of an (α, β)-expander: a network in which every set S of size at least $\alpha \cdot n$ has $|\Gamma(S)| \geq \beta|S|$. For what values of α can you say that G is an (α, β) expander for a constant β?

Q2.3. What is the maximum number of copies of a particular key that we have to make for this strategy? Give a high probability lower bound.

Q2.4. Suppose there was a restriction that no more than m copies of each key can be made. How could we change the distribution strategy so that the network formed is still an expander?