Randomized Algorithms 2013A – Problem Set 5

Robert Krauthgamer and Moni Naor

Date Due: February 13

Read Haeupler's paper [Hae11] and use it to answer the following questions in a self-contained manner. You are supposed to adapt or repeat proofs in the paper (or parts thereof), *without* explicitly citing or relying on it (e.g., you cannot just say that you apply Lemma 7 from the paper).

Throughout, let the network $G = (V, E)$ be a complete graph on n vertices. We consider the model of *random phone calls with push*, where rounds are synchronous, and at every round, each node independently chooses a random neighbor and send that neighbor a message of its choice.

1. Consider message forwarding, without any network coding. Specifically, there is only one original message $m \in \{0,1\}^\ell$, starting at a node $v \in V$. Once a node $w \in V$ receives the message, w forwards it (at every round) to a randomly-chosen neighbor.

   (a) Show that with probability at least 2/3, after $O(\log n)$ rounds, all nodes receive the message m.

   (b) Extend your analysis to the more general case where (i) every node stays silent independently with probability p, and (ii) the overall success probability is at least $1 - \delta$. You may assume that $0 < p, \delta \leq 1/2$.

2. Consider random linear network coding (RLNC) with k original messages $m_1, \ldots, m_k \in \{0,1\}^\ell$. More specifically, each relayed message comprises of k coefficients $\alpha_1, \ldots, \alpha_k \in \{0,1\}$ and the respective linear combination $\sum_{i \in [k]} \alpha_i m_i \in \{0,1\}^\ell$ (the computation is modulo 2). Thus, a relayed message has total length is $k + \ell$ bits. Each node's protocol is to send a vector chosen at random from the span of all its incoming messages (so far).

   Show that with probability at least 2/3, after $O(k + \log n)$ rounds, every node in the network can recover every original message m_i.

   Remark: For clarity, avoid the generic word "message", in favor of saying either *original message* or *encoded/relayed/incoming/outgoing messsage*. Similarly, distinguish between *knowing* an encoded message (whose meaning is as defined in the paper) and *recovering* an original message (which means that one can output this message).

References

[Hae11] Bernhard Haeupler. Analyzing network coding gossip made easy. In *Proceedings of the 43rd Annual ACM Symposium on Theory of Computing*, STOC 2011, pages 293–302. ACM, 2011. Available also from the author's webpage. doi:10.1145/1993636.1993676.