Algorithmic Aspects of Communication – Assignments
The University of Tokyo – Winter 2011
Instructor: François Le Gall

Choose at least **two of the three problems** below and solve all the questions in the problems you choose. Send your report to the instructor **before February 20th (5:00 PM)** by putting a copy in the instructor's mailbox located on the 1st floor of the Faculty of Science Building Number 7. Do not forget to write your name and your student number on the report.

Problem 1 (Communication Complexity)

(1) Let q be a prime number and let $GF(q)$ denote the finite field of size q. Suppose that Alice has input $x \in GF(q)$ encoded with $\lceil \log_2 q \rceil$ bits and Bob has input $y \in GF(q)$ encoded with $\lceil \log_2 q \rceil$ bits. Let $f_q \colon GF(q) \times GF(q) \to \{0,1\}$ be the function defined as

$$f_q(x,y) = \begin{cases} 0 & \text{if } x+y+xy = 0 \\ 1 & \text{if } x+y+xy \neq 0 \end{cases}$$

for all $x, y \in GF(q)$. Show that the randomized communication complexity of f_q is $O(\log \log q)$ bits. Can you prove a lower bound on the deterministic communication complexity of f_q?

(2) Let r be a positive integer and let V denote the vector space of dimension r over the finite field $GF(2)$. In other words, $V = \{0,1\}^r$, where the addition of two strings is done componentwise modulo 2. Suppose that Alice has as input a subspace $U \subseteq V$, and Bob has a vector $y \in V$. The goal is for Bob to decide if $y \in U$ or not. We suppose that only Alice can send messages to Bob, and that Alice wants to send as few communication as possible (this model is called *one-way communication complexity*). Construct a randomized communication protocol that solves (with high probability) this task using $O(r)$ bits of communication. (Hint: consider the orthogonal subspace $U^\perp$ of U.)

Problem 2 (Network Coding)

In Lecture 7 we focused on the multicast setting in network coding where all targets should receive the same information. Here we consider a slightly different setting called the *multiple unicast setting.*

(1) The graph of Figure 1 (sometimes called the *grail graph*) has two sources s_1, s_2 and two targets t_1, t_2. The goal is to send simultaneously one unit of information x (i.e., one element $x \in GF(q)$ for an arbitrary prime q) from s_1 to t_1, and one unit of information y from s_2 to t_2. Each edge in the graph is supposed to have unit capacity, i.e, one unit of information can be sent per edge. Design a protocol solving this task using the idea of network coding.

(2) The graph of Figure 2 has three sources s_1, s_2, s_3 and three targets t_1, t_2, t_3. The goal is to send simultaneously one unit of information x (i.e., one element $x \in GF(q)$ for some prime q) from s_1 to t_1, one unit of information y from s_2 to t_2 and one unit of information z from s_3 to t_3. Each edge in the graph is again supposed to have unit capacity. Design a protocol solving this task using the idea of network coding, for $q = 2$. More generally, for which other values of q does a protocol exist?

Problem 3 (Private Information Retrieval)

In lectures 10 and 11, we discussed information-theoretic private information retrieval. In the case of a single server, it was mentioned that any protocol must exchange $\Omega(n)$ bits of communication, where n is the size of the database owned by the server. Give a proof of this assertion (you are free to look at any book or research paper).

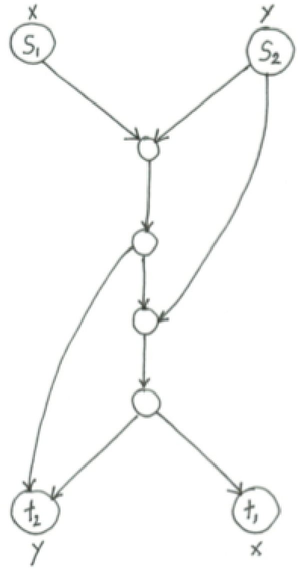

Figure 1: the grail graph

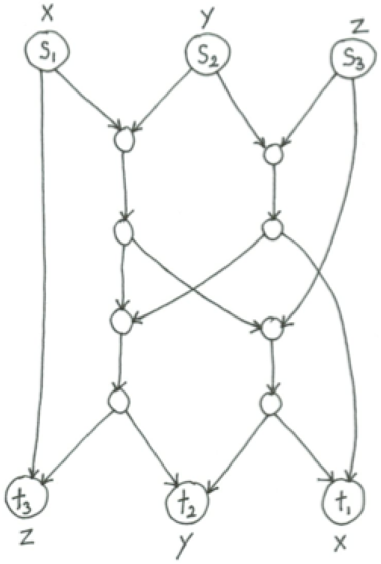

Figure 2: a three-source three-target graph