University of Freiburg
Dept. of Computer Science
Prof. Dr. F. Kuhn
P. Schneider

Advanced Algorithms
Problem Set 11

Issued: Tuesday, July 23, 2019

Exercise 1: Aggregation in the MPC Model

Assume you are given a number of $M \in \tilde{O}\left(\frac{N}{S}\right)$ machines (you may freely choose the hidden poly$(\log N)$ factor in the number of machines), where N is the number of *aggregation messages* that are collectively stored by the machines M_i, $i \in [M]$ and each machine M_i has a memory large enough to store S messages. We have $N \gg S$ and $S \in \tilde{\Omega}(1)$ (for a hidden poly$(\log N)$ factor of your choosing). By definition of the MPC model every machine can send and receive at most S aggregation messages.

Each aggregation message has encoded within it a target machine $i \leq N$. Additionally each aggregation message has a value associated with it. The *aggregation problem* is solved as soon as each machine learns an aggregation message that has *minimal* value among all aggregation messages of which it is the target. Carefully formulate a (randomized) algorithm that solves said aggregation problem in $O(\log N)$ and prove its correctness.

Hint: You may assume that messages have encoded within them the total number of messages with the same target. Machines have numbers $1, \ldots, M$ *that they are aware of. This allows that machine no. 1 computes and distributes public random bits (assume that you have arbitrary public randomness).*