Exam Distributed Algorithms

Vrije Universiteit Amsterdam, 31 May 2023, 18:45-21:30

(You may use the textbook Distributed Algorithms: An Intuitive Approach*. Use of slides, solutions to exercises, notes, laptop, calculator is* not *allowed.)*

(The exercises in this exam sum up to 90 points; each student gets 10 points bonus.)

1. Let the Dijkstra-Scholten algorithm be employed to detect termination of some centralized basic algorithm. Give an execution of the basic algorithm in which an active process q has a parent p in the Dijkstra-Scholten tree while q was made active for the last time by a process $r \neq p$. (10 pts)

2. Consider the weight-throwing termination detection algorithm with the counter $credit_p$ for recording weight, to avoid underflow. Why does an active process that receives a basic message not return this weight to the initiator immediately, but only after it has become passive? (10 pts)

3. Consider Franklin's election algorithm for undirected rings (with non-FIFO channels).

   (a) Give an example to show that an active process in election round n can receive a message for round $n+1$ before receiving the message for round n from this same direction, where these two messages carry different IDs. (8 pts)

   (b) Argue that it cannot receive a message for two rounds ahead. (12 pts)

4. Consider the Bracha-Toueg k-crash consensus algorithm, with $k < \frac{N}{2}$. Let more than $\frac{N+k}{2}$ processes choose the value b in the initial configuration. Argue that the correct processes will inevitably decide for b within three rounds. (10 pts)

5. Consider the heights (h_1, h_2) in the Walter-Welch-Vaidya mutual exclusion algorithm.

   (a) Argue that the minimum h_1-value in the network never decreases during computations. (8 pts)

   (b) Give an example where the minimum h_2-value in the network increases during a computation. (6 pts)

6. Suppose that in step 2 of the Kerberos authentication protocol, the authentication server would include the server ID S in the ticket it sends to the client. Explain how this would seriously hamper the applicability of the Kerberos protocol. (10 pts)

7. (a) Consider the Winternitz signature scheme with $k = 10$ and $\ell = 3$. Let 0100111010 be the hash of Alice's message to Bob. Explain how Alice signs her message, taking into account the checksum, and how Bob verifies this signature. (8 pts)

   (b) Suppose the Winternitz signature from (a) is placed in the third leaf of a binary Merkle tree of depth 4 and used by Alice in a Merkle signature of a message to Bob. Explain concretely what the signature looks like and how this signature is employed by Bob to verify whether the public key is genuine. (8 pts)