Online Exam Distributed Algorithms

Vrije Universiteit Amsterdam, 26 May 2021, 18:45-21:30

I declare to understand that taking an online exam during this corona crisis is an emergency measure to prevent study delays as much as possible. I know that fraud control will be tightened and realize that a special appeal is being made to trust my integrity. With this statement, I promise to make this exam completely on my own, only consult those sources that are allowed explicitly, not share my solutions with other students, and make myself available for any oral clarifications regarding this exam.

You can write your solutions with pen and paper. You are allowed to open the pdf's of the textbook and slides (only) at the following links. You are advised to open them in different tabs in your browser.

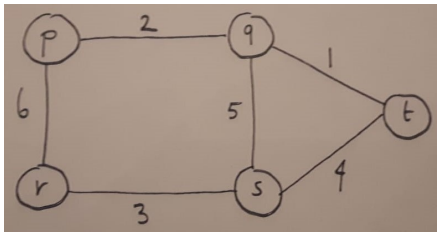
- `https://canvas.vu.nl/courses/53186/files/3745199`
- `https://canvas.vu.nl/courses/53186/files/3745089`

(The 6 exercises in this exam sum up to 90 points; each student gets 10 points bonus.)

1. Propose an adaptation of the Lai-Yang snapshot algorithm in which basic messages may be buffered at the receiving processes and the channel states of the snapshot are always empty. (14 pts)

2. Let Rana's algorithm be applied to an always terminating basic algorithm. Suppose a process at some point sends a basic message. Argue that there is a computation in which only this process calls *Announce*. (14 pts)

3. Give one possible computation of the Gallager-Humblet-Spira algorithm on the undirected weighted network below to determine a minimum spanning tree.



During the computation, the handling of the second **test** message from r to p should be delayed at p before it is rejected. (14 pts)

4. Consider the Afek-Kutten-Yung self-stabilizing algorithm for computing a spanning tree in an undirected network.

   (a) Suppose that at the start of the algorithm, all processes declare themselves root. Explain how this allows to simplify the algorithm. (8 pts)

   (b) Motivate why the resulting algorithm is not really self-stabilizing, in the sense that it should be able to cope with e.g. arbitrary bit flips at the hardware level. (8 pts)

5. Consider the time stamp approach to distributed transactions. Two transactions T_1 and T_2 run concurrently, with time stamps t_1 and t_2, respectively. Let variable x initially contain the value €10. T_1 writes the value €30 to x and then reads x, while T_2 reads x and then increases its value by €10.

   (a) Explain for all possible interleavings of the events of T_1 and T_2 whether T_1 and T_2 commit or abort. Distinguish two possible cases: $t_1 < t_2$ and $t_2 < t_1$. (8 pts)

   (b) Explain why in the case $t_2 < t_1$, aborts by T_2 are spurious. Propose an optimization of the time stamp approach that avoids these aborts. (8 pts)

6. (a) Consider the Winternitz signature scheme with $k = 10$ and $\ell = 3$. Let 1011000001 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 what the signature looks like and how this signature is employed by Bob to verify whether the public key is genuine. (8 pts)

After completing the exam, show your solutions to the camera before closing Proctorio.

After closing Proctorio, upload your solutions on Canvas, within 15 minutes.