Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Distributed Computing

Systems@ETH Zürich

Prof. T. Roscoe, Prof. R. Wattenhofer

Computer Systems

Quiz 2

Question 1

For byzantine agreement, when does all-same validity imply correct-input validity?

a) When there is only one byzantine node.

b) When the inputs are binary.

c) Both of the first two options are correct.

d) Neither of the first two options are correct.

Question 2

Suppose we shorten the king algorithm so that the nodes output their values after phase f instead of phase $f + 1$. What is the consequence of this?

a) The algorithm tolerates $f - 1$ byzantine nodes instead of f byzantine nodes.

b) The nodes fail to reach agreement with probability $\frac{1}{f+1}$.

c) Validity is lost.

d) All guarantees are lost.

Question 3

We have an asynchronous network that consists of 60 correct nodes and f byzantine nodes. If the nodes can reach byzantine agreement, what is the maximum possible value of f?

a) 19

b) 20

c) 29

d) 30

Question 4

In a network of 7 nodes where 3 nodes are byzantine, which of the following is the case when the nodes run the king algorithm with $f = 3$?

a) The algorithm works correctly.

b) The correct nodes might fail to agree.

c) Validity might not hold.

d) Both of the previous two options are correct.

Question 5

We are given a 10-round synchronous algorithm for byzantine agreement in a network of 1 billion nodes where 10 nodes are byzantine. Is it possible for the the algorithm to always succeed?

a) Yes.

b) No, but it is possible for it to always succeed if the byzantine nodes can only crash.

c) No, but it can succeed with a high probability using randomization.

d) Both of the previous two options are correct.

Question 6

In a network of n nodes where a fixed set of f nodes are byzantine, we run a version of the king algorithm where in each phase the king is chosen uniformly at random. After k phases, which is the tightest upper bound for the probability that the nodes fail to reach agreement?

a) $\frac{f}{k}$

b) $\frac{f}{kn}$

c) $\left(1 - \frac{f}{n}\right)^k$

d) $\left(\frac{f}{n}\right)^k$

Question 7

In a network of n nodes where f nodes are byzantine, how many rounds in expectation does it take for the Ben-Or algorithm to terminate?

a) a constant number of rounds

b) $\Theta(n)$ rounds

c) $\Theta(c^n)$ rounds for some constant $c > 1$

d) The answer depends on both n and f.

Question 8

In a network of n nodes where f nodes might crash, each node i broadcasts its input x_i, and outputs the first value it receives from $n - 2f$ nodes (or waits forever). Which of the following is the tight inequality which guarantees that all outputs are equal?

a) $n > 3f$

b) $n > 4f$

c) $n > 5f$

d) $n > 6f$

Question 9

Which of the following statements about Bracha's algorithm is FALSE?

a) It can tolerate $f < n/3$ Byzantine failures.

b) It requires a constant number of rounds.

c) It requires synchrony to handle a Byzantine sender.

d) Its communication complexity exceeds the lower bound by $\Theta(n)$.

Question 10

Let us redefine reliable broadcast so that one of the properties totality, agreement, or validity is no longer required. Dropping which property makes a zero-communication algorithm possible? Note that we still require integrity.

a) Dropping just one of these three properties is not enough for zero communication.

b) Totality

c) Agreement

d) Validity

Question 11

We want a reliable broadcast algorithm where if the sender crashes and fails to broadcast any input, then the correct nodes all output $\perp$. What is required for this?

a) The network must be synchronous.

b) The algorithm must be randomized.

c) Both of the first two options are correct.

d) Neither of the first two options are correct.

Question 12

We run the efficient reliable broadcast algorithm 18.22 with one change: We use an $(n, 1)$-erasure code instead of an $(n, f + 1)$-erasure code. What is the consequence?

a) The algorithm no longer terminates because now the nodes need n fragments instead of $n - f$.

b) The algorithm loses the agreement property because now 1 byzantine node is enough to prevent agreement.

c) The algorithm becomes less efficient because the fragments become larger.

d) All previous options are FALSE.

Question 13

In a network of n nodes, is reliable broadcast for any input of size L possible with $0.5nL + \mathcal{O}(kn^2 \log n)$ bits of communication, where k is the length of a cryptographic hash?

a) No, because at least $\Omega(Ln^2)$ communication is required.

b) No, but $\mathcal{O}(Ln + kn^2 \log n)$ communication is sufficient for reliable broadcast.

c) Potentially yes, though this communication complexity has not been achieved so far.

d) Yes, and this is the communication complexity of the best known algorithm.

Question 14

Given a merkle tree with 2^k leaves, how many hashes are required to prove that a leaf belongs to the tree assuming the root hash is known?

a) $\log_2(k)$

b) k

c) $k + 1$

d) $2k + 1$

Question 15

In a network of 10 correct nodes and no byzantine nodes, each node reliably broadcasts its input to the other nodes using Algorithm 18.11. At most how many messages (including to themselves) do all the nodes send together in total?