Byzantine Agreement Task

Read the article by Joseph Y. Halpern (USING REASONING ABOUT KNOWLEDGE TO ANALYZE DISTRIBUTED SYSTEMS, Ann. Rev. Comput. Sci. 1987, 2: 37-68) carefully and answer the following questions:

1. On page 43 a definition of common knowledge is given. Why is this idea important? What could be possible applications using the idea of common knowledge?

2. Consider Figure 1 on page 42. Which proposition(s) (including the tautology) is (are) common knowledge in s, t, or u? Give an argument for your decision.

3. Using the definition of common knowledge, given on page 43, prove the following "fixpoint" equation (the underlying logic is S5):

$(M, s) \models C_G\varphi$ iff $(M, s) \models E_G(\varphi \wedge C_G\varphi)$ [$E_G(\varphi)$ is an abbreviation for $\forall(i \in G)\, K_i(\varphi)$]

4. Explain how the coordinated attack problem (p. 47 ff) relates to the task of establishing common knowledge.

5 Compare the simultaneous Byzantine agreement problem as described on page 54 ff with the traditional formulation given here:

> **Byzantium, 1453 AD.** The city of Constantinople, the last remnants of the hoary Roman empire, is under siege. Powerful Ottoman battalions are camped around the city on both sides of the Bosporus, poised to launch the next, perhaps final, attack. Sitting in their respective camps, the generals are meditating. Because of the redoubtable fortifications, no battalion by itself can succeed; the attack must be carried out by several of them together or otherwise they would be trusted back and incur heavy losses that would infuriate the Grand Sultan. Worse, that would jeopardize the prospects of a defeated general to become Vizier. The generals can agree on a common plan of action by communicating thanks to the messenger service of the Ottoman Army which can deliver messages within an hour, certifying the identity of the sender and preserving the content of the message. Some of the generals however, are secretly conspiring against the others. Their aim is to confuse their peers so that an insufficient number of generals is deceived into attacking. The resulting defeat will enhance their own status in the eyes of the Grand Sultan. The generals start shuffling messages around, the ones trying to agree on a time to launch the offensive, the others trying to split their ranks...

Use the traditional formulation and explain what it means that the underlying communication mechanism is

- *synchronous*
- *searching for agreement*
- *point-to-point (connected)*

6. The situation above describes a classical coordination problem in distributed computing known as *Byzantine agreement* which was introduced in two seminal papers by Lamport, Pease and Shostak[1]. Broadly stated, a basic problem in distributed computing is this: Can a set

[1] L. Lamport, R. Shostak, and M. Pease, The byzantine generals problem, ACM Trans on Prog Lang and Syst, Vol. 4, 382-401, 1982. M. Pease, R. Shostak, and L. Lamport, Reaching agreement in the presence of faults, J. ACM, Vol. 27, 228-234, 1980.

of concurrent processes achieve coordination in spite of the faulty behaviour of some of them? Give a short summary of the main results as discussed in the paper (page 55 ff).

7. Explain what is expressed by the following "fixpoint" property (Page 56):

$(R, r, t) \models C_N\varphi$ iff $(R, r, t) \models E_N(\varphi \wedge C_N\varphi)$?

8. Consider statements of the form $(R, r, t) \models C_N\varphi$. Give an explicit example for φ where this statement is true!

9. The protocol on top of page 57 is an example of a knowledge-based protocol and it is claimed to be an optimal protocol for solving the *Byzantine agreement task* in case of crash failures and omission failures.
a. What is a knowledge-based protocol?
b. What are crash failures and omission failures?
c. What are Byzantine errors and why is their analysis more difficult?

10. Consider 4 processors, of which 1 is a faulty processor (crash and omission failures only). Construct an explicit example showing how the protocol on top of page 57 could be applied. Assume the following three initial situations: 0000, 1111, and 1010. Specify each round regarding the actions of the processor (indicating when a processor is failing). State also at what rounds new common knowledge is established regarding the group of non-faulty processors.

11. P. 58: Given that the presented knowledge-based protocol is optimal, Halpern states that it can be converted to a standard protocol by removing the tests for knowledge. Explain the main ideas of how to convert a knowledge-based protocol into a standard protocol in case of crash failures.