Choice Coordination and Byzantine Agreement

Feedback Report Randomized Algorithms IN4337

Koos van der Linden
4133145

Marieke van der Tuin
4079299

1. STRUCTURE

We have several remarks on the structure of the report. The report is readable on its own, which is good. The problem is introduced and variables are explained.

The report begins with an introduction that has little use. An introduction should contain at least a motivation. Section 2 should explain the problem and the model, which it does properly. But this section also contains other information such as the running time of the algorithms that are yet to be introduced. Furthermore it mentions the running time of a deterministic algorithm for the choice coordination problem (CPP): such facts should be in the introduction. This is true for a large part of section 2.

The included pseudo-code in section three is very useful. It is sufficient to understand the algorithm. A little more explanation of the use of variables could be useful, for example the difference between C_i and R_i is not explained.

Before the experimental results are shown, an explanation of the experimental method should be included. What is measured, and why is this measured? The plots that are included are clear. The box-plot in figure 1 could have been left out, it doesn't give extra information.

We would suggest that section 5 should follow up section 3. It is in our opinion better to start with the theoretical analysis and than compare this with the experimental results. Then questions can be answered like ”are the results as expected?”.

In section 2 it is mentioned that a deterministic algorithm for CPP exists with running time $\Omega(n^{\frac{1}{3}})$. For the Byzantine Agreement (BA) a deterministic algorithm exists that requires $t+1$ round. No further reference is made to this. This is not compared with the running time of the randomized algorithm. The discussion of the benefit of randomization is missing in the report.

We also miss the comparison of the results with the theoretical analysis in section 5 and the constant running time and success probability mentioned in section 2. No conclusions are drawn from the experimental results, the results are not even discussed.

Section 5, the analysis, is done neatly. This section gives an answer to Exercise 12.20 and 12.21 and to problem 12.27.

2. CHOICE COORDINATION PROBLEM

For CPP we have several concerns. First of all, the algorithm for ASYNCH-CPP is given, but it is not analysed. It is said that the analysis for SYNCH-CCP also holds for ASYNCH-CCP. But ASYNCH-CPP is not tested, nor discussed, nor shown that it is equal to SYNCH-CPP, so we are not convinced. Is it even implemented?

In section 2 the probability of success of CPP is mentioned, but this is not explained. In the results this success probability is not tested. And what conclusions can be drawn from the fact that the number of iterations closely resemble a geometric distribution with $p = \frac{1}{2}$?

In [1] $n = m = 2$ is chosen to keep the analysis of SYNCH-CPP simple. In this report no theoretical analysis of SYNCH-CPP is included. But in the runtime analysis of SYNCH-CPP this choice $n = m = 2$ is also made. Why is this done? It would be interesting to see the performance of the algorithm for other values. Secondly, it is stated that the algorithm requires a constant number of steps. But because the algorithm is tested for only one value of n, this is not shown from the experimental results.

3. BYZANTINE AGREEMENT

In section 2, it is said that ByzGen runs in constant time, but this is not shown at the experiments. In the results it is shown for $t = n/4$, for several values of n, according to the first experiment where this seems to be the border of good vs bad results. In the theoretical analysis it is said that the algorithm only works for values $t < n/6$, and with the choice of L, H, and G, $t = n/8$ would be expected. No conclusion is drawn from the fact that this behaviour does not agree with the analysis. If according to the analysis the algorithm should not work for these values, why do the results show else?

In section 3, the choice of L, H, and G for ByzGen is not explained, nor are these variables explained. It is not clear for us what these variables mean. The chosen values are taken from [1]. Also as mentioned in section 5, algorithm 3 does not stop. It would be helpful if section 3 referred to section 5 for the halting procedure.

In all figures in the experimental results, the algorithms are run multiple times to derive averages, which is good. In figure 5 it does not seem that the algorithm is run more than once per value of n. We would recommend to do so.

In [2] the ByzGen was originally published ([1] refers to this paper). This report does not refer to this paper. In [2] it is shown that with a correct choice of L, H, and G, the best bound to get is $t < n/4$, although the report claims that this bound cannot be better than $t < n/6$. We think that this conclusion is drawn wrongly from the last part of section 5.

In [2] several other interesting conclusions are drawn. For instance the maximum number of messages in ByzGen is max $O(n^2)$. This could have been taken into account in the experimental analysis.

4. GENERAL ASSESSMENT

Our first impression of the report was positive. The report was easy to read; the explanation of the problems, the experiment, and the theoretical analysis was done well. When we started to look more carefully, there arose some concerns. CPP is not tested well enough, and not discussed theoretically. The theoretical analysis in section 5 is done neatly, but the conclusion is not correct according to [2]. We would expect the authors to have read this paper.

5. REFERENCES

[1] R. Motwani and P. Raghavan. *Randomized algorithms.* Cambridge University Press, Cambridge, UK, 1995.

[2] M. O. Rabin. Randomized byzantine generals. In *Foundations of Computer Science, 1983., 24th Annual Symposium on*, pages 403–409. IEEE, 1983.