Comments on "Capacity of Byzantine Agreement"*

Guanfeng Liang and Nitin Vaidya
Department of Electrical and Computer Engineering, and
Coordinated Science Laboratory
University of Illinois at Urbana-Champaign
gliang2@illinois.edu, nhv@illinois.edu

Technical Report

January 29, 2010

In our previous work [1] we proposed an algorithm to achieve Byzantine agreement in a four node network at rate of R given that a set of link capacity constraints are satisfied (Inequalities 2 to 16 in [1]). Recently, we discovered that only inequalities 2 to 13 are necessary. Moreover, we also found that they are also sufficient if the inequalities are strict. We are able to prove the sufficiency of the strict inequalities by construction. In particular, we introduced an agreement algorithm that achieves agreement throughput arbitrarily close to R.

1 Capacity of the Four Node Network

Consider the same four node network in [1]. Figure 1 shows the four-node network. The labels near the various links denote the link capacities. Without loss of generality, we assume that $k \leq l \leq m$.

The the following constraints are necessary for agreement throughput of R to be achievable:

- If one of the peers is removed from the network, then these conditions must be true for the min-cut from S to a remaining peer to be at least R:

$$k + l \geq R \tag{1}$$

*This research was supported in part by Army Research Office grant W-911-NF-0710287

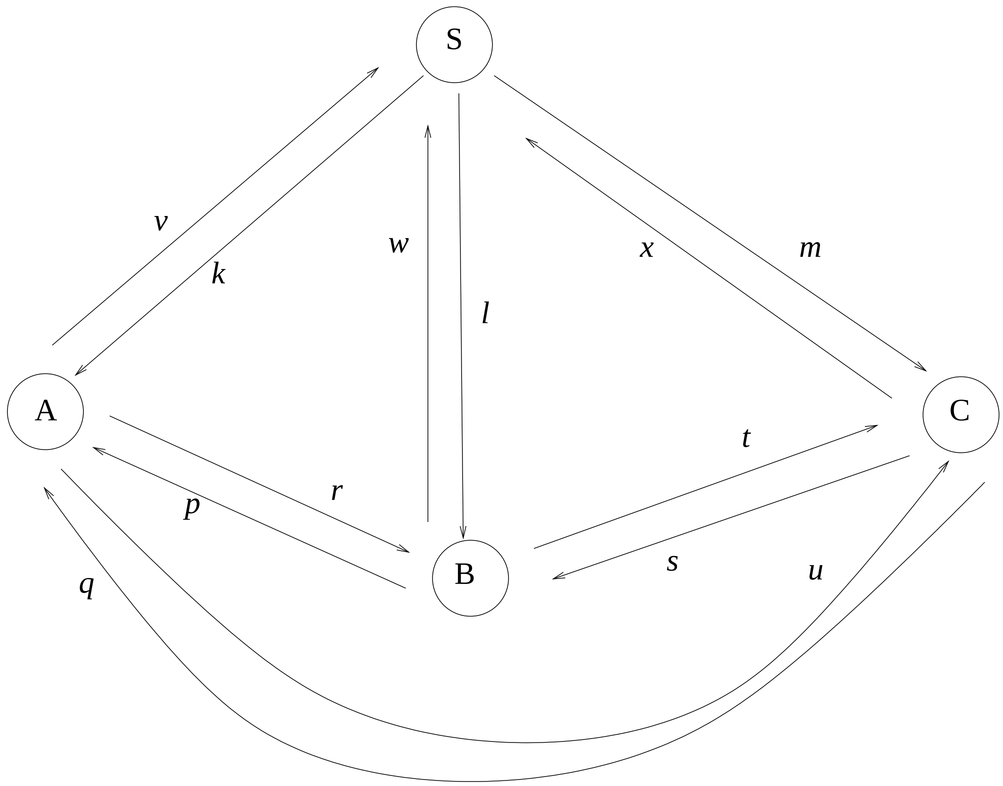

Figure 1: Four node network: Labels denote the link capacities. Without loss of generality, we assume that $k \leq l \leq m$.

$$l + m \geq R \tag{2}$$
$$m + k \geq R \tag{3}$$
$$p + k \geq R \tag{4}$$
$$q + k \geq R \tag{5}$$
$$r + l \geq R \tag{6}$$
$$s + l \geq R \tag{7}$$
$$t + m \geq R \tag{8}$$
$$u + m \geq R \tag{9}$$

- The max-flow to one of the peers from the other two peers, with sender S removed, must be at least R.

$$p + q \geq R \tag{10}$$
$$r + s \geq R \tag{11}$$
$$t + u \geq R \tag{12}$$

The necessity of the above conditions are already shown in [1]. The proof of sufficiency when the inequalities are strict will be released later this year.

References

[1] N. Vaidya and G. Liang, "Capacity of byzantine agreement (preliminary draft - work in progress)," *Technical Report, CSL, UIUC*, January 2010.

[2] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," *ACM Transactions on Programming Languages and Systems*, vol. 4, pp. 382–401, 1982.

[3] M. Pease, R. Shostak, and L. Lamport, "Reaching agreement in the presence of faults," *JOURNAL OF THE ACM*, vol. 27, pp. 228–234, 1980.