York University CSE 6117 October 15, 2008

Homework Exercise #4
Due: October 29, 2008

4. Consider the algorithm we studied in class that solves consensus tolerating up to f Byzantine failures in a complete synchronous network of n processes when $n > 4f$. It satisfies the following two properties:

- Agreement: Every correct process outputs the same value.
- Weak validity: If every correct process has input v, then every correct process outputs v.

In the questions below, we also consider a stronger version of the validity property:

- Strong validity: The output of each correct process is the input of some correct process.

(a) Show that the assumption that $n > 4f$ is really crucial for that algorithm's correctness. In other words, for every $n \leq 4f$, construct an execution that violates the correctness properties.

(b) Prove that, in general, the algorithm does not satisfy strong validity.

(c) Consider the binary consensus problem, where inputs are drawn from the set $\{0, 1\}$. Give a *simple* way of modifying the algorithm so that it satisfies agreement and strong validity for this special case. Explain why your answer is correct.