York University CSE 6117 February 3, 2016

Homework Assignment #4
Due: February 12, 2016 at 3:00 p.m.

1. Consider the algorithm we studied in class that solves Byzantine agreement tolerating up to f Byzantine failures in a complete synchronous network of n processes when $n > 4f$. Inputs to the algorithm can be any integers. The algorithm 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 agreement or weak validity.

(b) Show that the algorithm does not guarantee strong validity even when $n > 4f$.

(c) Suppose that inputs of correct processes can come from the set $\{1, 2, 3, 4\}$. Prove that no algorithm can guarantee strong validity and agreement when $n = 12$ and $f = 3$.