York University CSE 6117 October 25, 2009

Homework Exercise #5
Due: November 3, 2009

1. Consider a synchronous message-passing system of n processes. The network graph is complete. Up to f processes may experience Byzantine failures.

Consider the problem of (binary) majority Byzantine consensus, where each process gets a single bit as input and the following three properties must be satisfied:

- Termination: Each correct process must eventually produce an output.
- Agreement: Two correct processes never output different values.
- Majority validity: If at least two thirds of the correct processes have the same input value v, then all correct processes output v.

(a) Find a constant c such that the problem is unsolvable whenever $n \leq cf$. (The bigger your c, the better.)

(b) Recall the algorithm discussed in class that uses $f + 1$ phases, each with 2 rounds, to solve binary Byzantine consensus when $n > 4f$. Make small modifications to this algorithm so that it solves majority consensus when $n > df$ for some constant d. (The smaller your d, the better.)