

Byzantine Generals Algorithm (Lamport, Shostak, and Pease, 1982)

Defined recursively on m.

function majority(v_1, v_2, \dots, v_p)
 return majority value or RETREAT if no majority exists

Base case:

BG_Send(0,v,L)
 Send v to every lieutenant in L

BG_Recv(0)
 Return value sent to you, or RETREAT if no message received

Recursive case (m > 0):

BG_Send(m,v,L)
 Send v to every lieutenant in L

BG_Recv(m)
 Let v be value sent to you, or RETREAT if no message received
 Let L be set of lieutenants who have never broadcast v
 BG_Send(m-1,v, L-{self})
 Use **BG_Recv**(m-1) to receive v_i for every i in L - {self}
 Return majority(v, $v_{i1}, \dots, v_{i(|L|-1)}$)