Exercise 6

1 Epidemic Probabilistic Broadcast

Consider the system model with n servers, of which some number t may crash. When n is large (thousands or even millions), protocols of the kind we have considered perform poorly, because a single server needs to send messages to and receive messages from all others.

An alternative are *epidemic* protocols for reliable broadcast, where the sender sends its message to a small randomly chosen subset of αn servers, who in turn forward the message to another randomly chosen set of αn, etc. This process continues for a number of k rounds, until every message has been forwarded k times.

Since there will be runs where not all servers deliver the message, the *validity* and *agreement* conditions of reliable broadcast have to be weakened. The conditions are replaced by the following:

Probabilistic validity: There is a constant ϵ such that for any two correct servers P_i and P_j, when P_i *r-broadcasts* a message m, then P_j *r-delivers* m with probability at least $1 - \epsilon$.

The integrity property of reliable broadcast remains unchanged.

Tasks:

a) Formalize a protocol for epidemic reliable broadcast.

b) Derive a lower bound on the probability that s servers have r-delivered a message r-broadcast by a correct sender after k rounds. (Use Maple or Mathematica to plot it for some values of α.)