Buffer as Circular Array
Hoare-Style Proof of Correctness

0 ≤ size ∧ size ≤ max_size ∧ ibuffer[1..maxsize] ∧
1 ≤ bot ∧ bot ≤ maxsize ∧ 1 ≤ top ∧ top ≤ maxsize

{PROCEDURE BufferIn(x:X; VAR report:ReportType);
    top.in := top; bot.in := bot; size.in := size;
    max_size.in := max_size; ibuffer.in := ibuffer;
    IF size < max_size THEN
        BEGIN
            size := size + 1;
            top := (top MOD max_size) + 1;
            ibuffer[top] := x;
            report := OK
        END
    ELSE report := full; }

(size.in < max_size) ∧
    max_size = max_size.in ∧
    bot = bot.in ∧
    0 ≤ size ∧
    size = size.in + 1 ∧
    top = (top.in mod max_size.in) + 1 ∧
    ∀i{ i ≠ top ⇒ ibuffer[i] = ibuffer.in[i] } ∧
    buffer[top] = x ∧
    report = OK)
∨ (size.in = max_size ∧
    max_size = max_size.in ∧
    bot = bot.in ∧
    top = top.in ∧
    size = size.in ∧
    ibuffer = ibuffer.in ∧
    report = full)