Conventions

- `1(P)`, for a predicate `P`, denotes the *indicator* function of `P`, i.e., `1` if `P` holds and `0` otherwise.
- $X_{i,j}$ denotes $(X_i$ and $X_j)$
- $X_{i..j}$ denotes $(X_i$ and X_{i+1} and $\cdots$ and $X_j)$
- X satisfies invariance rule means
  - initialization establishes X
  - every atomic rule unconditionally preserves X
- X satisfies invariance rule given Y means
  - *Inv* Y holds
  - initialization establishes Y
  - every atomic rule unconditionally establishes $Y \Rightarrow X$ starting from Y and X

Part a

Define the following predicates:

B_0 : α01 + α10 + 1(done) = 1 // exactly one of the terms equals 1 and the others equal 0
B_1 : union(s0.bg, s1.bg, α01, α10) = union(B0, B1) // the elements of B0 and B1 are preserved
B_2 : s1.bg.size = B1.size
B_3 : s0.bg.size + α01 + α10 = B0.size
B_4 : α10 $\neq$ [] $\Rightarrow$ α01.head $\leq$ min(s1.bg) // is it ok to write B_4 as: α10.head = q $\Rightarrow$ q $\leq$ min(s1.bg)
B_5 : (done $\Rightarrow$ max(s0.bg)) $\leq$ min(s1.bg)

$B_{0..5}$ satisfies the invariance rule and implies A_0

More detail on how $B_{0..5}$ satisfies invariance rule

Each of B_0, B_1, B_2 and B_3 (individually) satisfies the invariance rule.
B_4 satisfies the invariance rule given *Inv* B_0. (Where is B_0 used?)
B_5 satisfies the invariance rule given *Inv* B_4.

More detail on how $B_{0..5}$ implies A_0

$B_{0..3}$ and done imply s0.bg.size = B0.size, s1.bg.size = B1.size, and α01 and α10 are empty.
This and B_5 imply A_0.

Part b

Consider the following function:

G : sum(union(s0.bg, α01, α10)) // sum of integers in s0.bg, α01 and α10

The following hold:

L_1 : ($G = k$ and α01$\neq$[]) *leads-to* (α10$\neq$[] and ($G < k$ or α10.head $\geq$ max(s0.bg))) // via s1.receive
L_2 : ($G = k$ and α10$\neq$[]) *leads-to* (($G = k$ and α01$\neq$[]) or done) // via s0.receive
L_3 : (α10$\neq$[] and α10.head$\geq$max(s0.g)) *leads-to* done // via s0.receive
C_0 : *Inv* $G \geq 0$

So G is almost there; just need to augment it to handle L_2 and L_3 For brevity, define

H : α10$\neq$[] and α10.head$\geq$max(s0.g)

The following function works

F : [G –1(H), α10.size]