Condition I2 and Stuttering

Condition I2 doesn't really show that every step of the algorithm leaves *Inv* true; it just shows that every *Next* step does. Our specification also allows stuttering steps—ones that leave all the specification's variables unchanged. We should also show that executing a stuttering step when *Inv* is true leaves *Inv* true. That is, instead of proving I2, we should prove

I2a. $Inv \land [Next]_{vars} \Rightarrow Inv'$

where *vars* is the tuple of all variables. But since the specification's variables are the only ones that occur in *Inv*, a stuttering step executed when *Inv* is true obviously leaves *Inv* true. Hence, I2 implies I2a. We therefore often ignore stuttering steps when reasoning about invariance and just prove I2.

CLOSE