Manna and Pnueli approach exercises

The aim of this assignment is to exercise with the Invariance and Progress proof rules as presented in the handouts from the Manna and Pnueli (MP) approach. The idea is, to re-do some of their proofs for the somewhat simpler (as opposed to the MP-approach) representation of systems used in the lecture notes:

1. Locations in a system are indicated by interpreting the names as propositions which are true iff control is at such location, e.g., n1, t1, . . .

2. Transitions are indicated by their source/target names, e.g., n1t1, t1c1, . . .

As in MP, assume that idle transitions are present at all locations.

Four proofs are asked for, each one provides 7 points - together with 2 for free this provides 30 points.

1. For the MUTEX algorithm as given in the lecture notes (with the signature variable) provide the proof for Mutual Exclusion using the rule INV (this involves providing the appropriate invariant).

2. For the MUTEX algorithm as given in the lecture notes (with the signature variable) provide the incremental proof for Mutual Exclusion using either the ”Strategy 2” approach on pp 97-94 or using the rule INC-INV (this involves providing several supporting invariants).

3. For the MUTEX algorithm as given in the lecture notes (with the signature variable), indicate and motivate which transitions should be in the Justice set to achieve Eventual Access. Provide the proof for Eventual Access using the rule CHAIN-J.

4. For the MUTEX algorithm without the signature variable, i.e., with the transition t1c1 to the critical section c1 guarded by only ¬c2 (and vice versa) as given in the lecture notes, indicate and motivate which transitions should be in the Justice set and which ones in the Compassion set to achieve Eventual Access. Provide the proof for Eventual Access using the rule CHAIN-F.

NB The exercises are quite easy and similar to the ones in the book, so the challenge is in the detail: solutions should be carefully argued and proofs for, e.g., temporal clauses in the rule CHAIN-F should be provided. Also, invariants should be introduced and motivated where required in the proof; this may involve some re-ordering of the proof steps as given in the handouts.