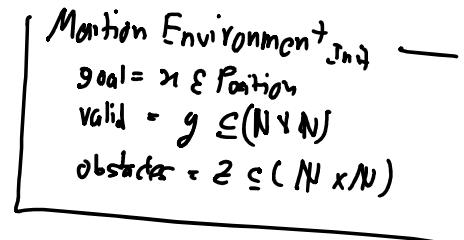
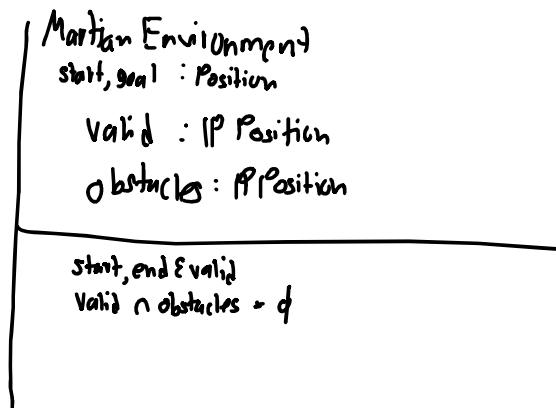


If the world pauses right now, the following facts will hold true:

- There is a Martian environment that is made of:
  1. A starting point
  2. A goal point
  3. Obstacles (except at the goal location)
  4. 1 master rover
  5. 2 side rovers
  6. Any other point

$N, M : \mathbb{N}$   
 $\text{Position} := (0 \dots N-1) \times (0 \dots M-1)$



### Rover-Related Facts

- There is a master rover at some point in the Martian environment
- The master rover is not located on:
  - an obstacle
- The master rover has a battery level between 0 (non-inclusive) and a maximum value

The master rover is in exactly one of the following states:

### 1. Failed (Failure Mode)

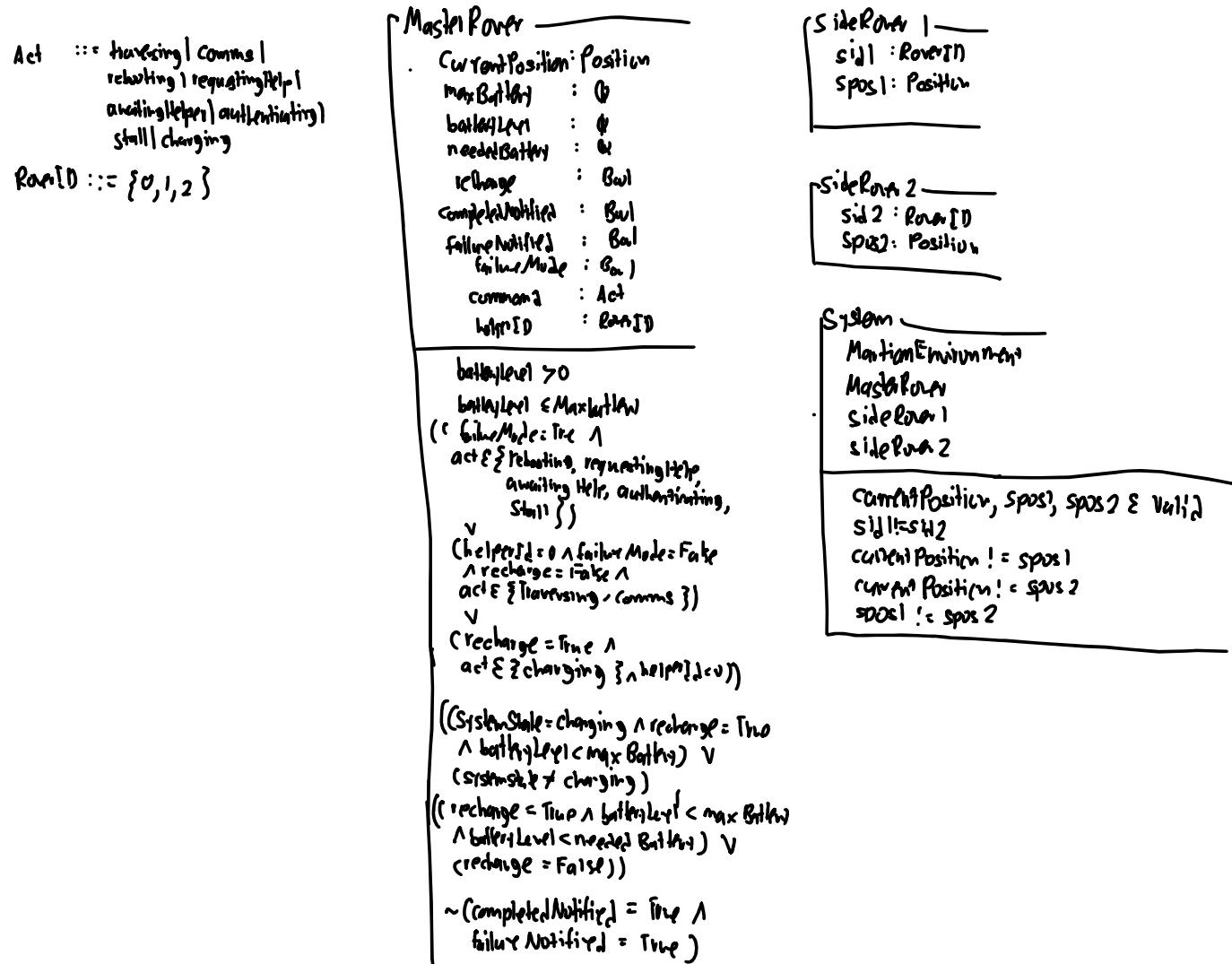
- Rebooting
- Requesting help
  - Notify ground station
  - Awaiting side rover arrival
  - Authenticating a side rover  
(e.g. establishing communication between rover IDs)

### 2. OK

- Traversing
- Setting up communication with ground control at goal location

### 3. Charging (Recharge Mode)

- Battery is not at maximum



### MasterPower<sub>Tail</sub>

CurrentPosition =  $\lambda \in P(N \times N)$   
 MaxBattery =  $\lambda \in Q_{>0}$   
 batteryLevel =  $\lambda \in Q_{>0}$   
 isCharge = False  
 completeMobilized = False  
 failureNotify = False  
 failureMode = Free  
 commProg = Transferring  
 helpSd = 0

### SidePower 1<sub>Tail</sub>

sid1 =  
 Spos1 =  $\lambda \in P(N \times N)$

### SidePower 2<sub>Tail</sub>

Sid2 = 2  
 Spos2 =  $\lambda \in P(N \times N)$

### System<sub>Tail</sub>

MontionEnvironment<sub>Tail</sub>  
 MasterPower<sub>Tail</sub>  
 SidePower 1<sub>Tail</sub>  
 SidePower 2<sub>Tail</sub>

Move —  
Δ Master Rover

nextPosition

command = traversing  
recharge = False  
failureMode = False  
nextValid  
currentPosition = next  
batteryLevel = batteryLevel - 1  
neededBattery = neededBattery - 1

SL4: rover does not collide with obstacles because currentPosition and next are in valid

G7: Rover is stationary when charging

G7: FailureMode entered

Begin Failure —  
Δ Master Rover

failureMode = True  
failureMode' = True  
command' = still

Attempt Reboot —  
Δ Master Rover

failureMode = True  
Command' = Rebooting

Reboot Success —  
Δ Master Rover

failureMode = True  
Command = Rebooting  
SystemState' = ok  
command' = traversing

Reboot Fail —  
Δ Master Rover

failureMode = True  
Command = Rebooting  
SystemState' = Failure  
command' = Requesting Help

SL3: rover either reboots or request help on failure.

Attempt Request Help —  
Δ Master Rover

failureMode = True  
Command' = Requesting Help

NotifyFailure —  
Δ Master Rover  
Δ idle Rover 1  
Δ idle Rover 2

command = Requesting Help  
helperId = 0  
failureNotified' = True  
Command' = awaitingHelp  
helperId' ∈ {sid1, sid2}

Failure Solv'd —  
Δ Master Rover

failureMode = True  
(0, command') = traversing  
helperId' = 0  
failureMode' = False

G7: Recharge set to True

Initiate Recharge —  
Δ Master Rover

recharge = False  
batteryLevel < maxBatteryLevel  
batteryLevel < neededBattery + recharge'  
recharge' = True

chargeUptick —  
Δ Master Rover

recharge = True  
batteryLevel < maxBatteryLevel  
batteryLevel' = batteryLevel + 1

Begin Recharge —  
Δ Master Rover

recharge = True  
Command' = Charging

EndRecharge —  
Δ Master Rover

recharge = True  
batteryLevel = maxBattery  
command' = traversing  
recharge' = False

G7: Charging ends when battery full

G6: notification sent on reaching goal

Goal Reached —  
Δ Master Rover

currentPosition = goal  
Command = command  
CompletedNotify' = False  
Command' = Command

Notify Completed —  
Δ Master Rover

currentPosition = goal  
Command = command  
CompletedNotify' = True

