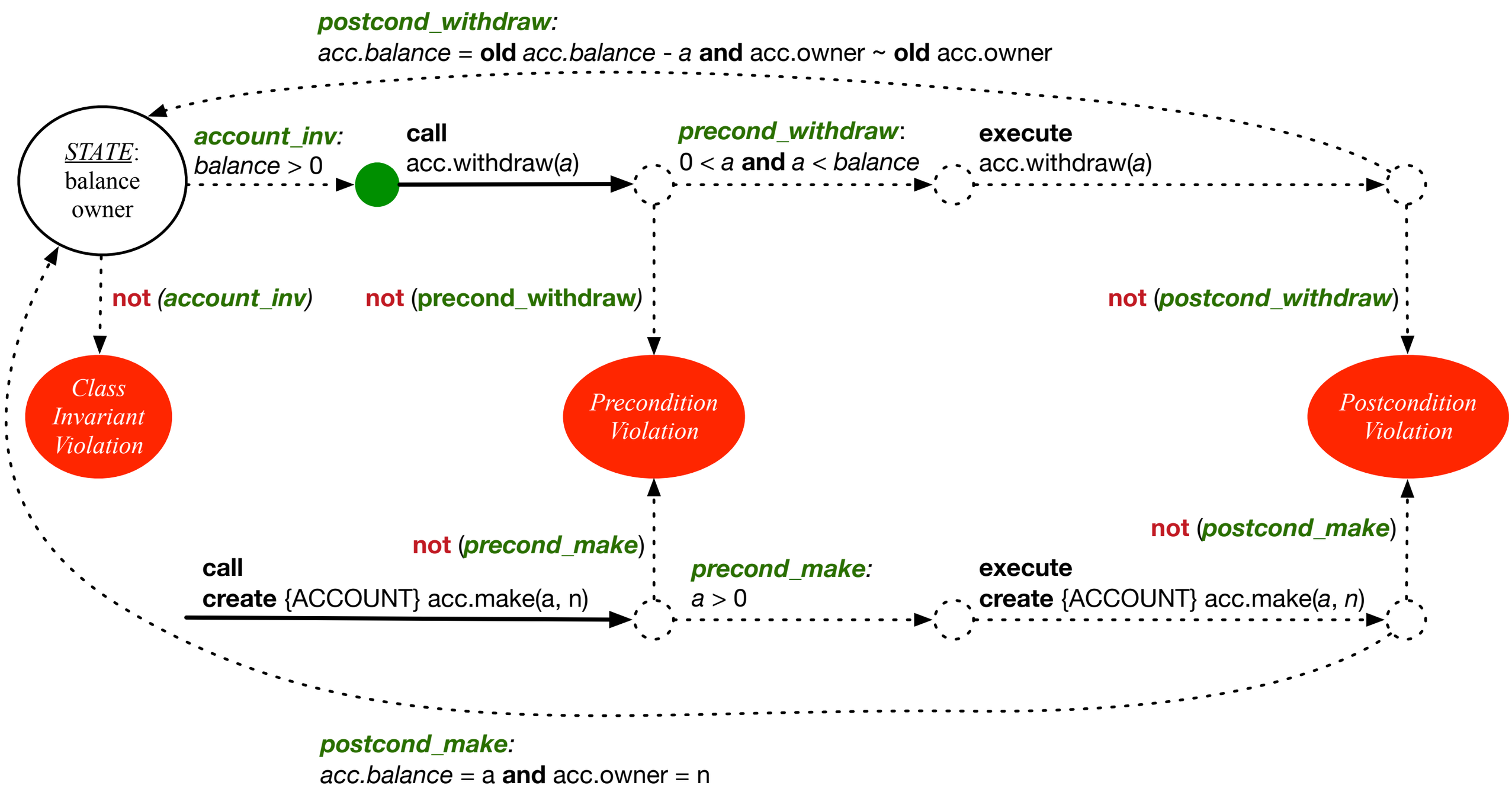
postcond_withdraw:
acc.balance = old acc.balance - a and acc.owner ~ old acc.owner
STATE:
balance
owner
account_inv:
balance > 0
call
acc.withdraw(a)
precond_withdraw:
0 < a and a < balance
execute
acc.withdraw(a)
not (account_inv)
not (precond_withdraw)
not (postcond_withdraw)
Class Invariant Violation
Precondition Violation
Postcondition Violation
not (postcond_make)
not (precond_make)
call
create {ACCOUNT} acc.make(a, n)
precond_make:
a > 0
execute
create {ACCOUNT} acc.make(a, n)
postcond_make:
acc.balance = a and acc.owner = n