ADT Exercise Solution

Prove balance always returns non-negative value

Base case: balance (new_account (o)) >= 0
Step case: Assume balance (e) >=0 where e is of n nested levels
Prove that balance (e')>=0 where expression e' is of n+1 nested levels

Prove:
Base case: balance(new_account(o))>=0 axiom 1

Step case:
e' can be of either form: deposit (e, v) or withdraw (e, v)

Case 1: e' is deposit (e, v)

balance (deposit (e, v)) = balance (e) + v	axiom3
balance (e)>=0	induction hypothesis
v>=0	precondition of deposit
balance (e) + v >=0	

Case 2: e' is withdraw (e, v)

balance (e') = balance (withdraw (e, v))	axiom 4
balance (e) >=0	induction hypothesis
v>=0 and balance (e)>=v	precondition of withdraw
balance (e) – v >=0	

QED

How to find out missing specification?

Using existing axioms, can we decide the value of:

owner (deposit (*a, v))*

owner (withdraw (*a, v))*

So we add the following:

owner (deposit (*a, v)) = owner (a)* *(axiom 5)*

owner (withdraw (*a, v)) = owner (a)* *(axiom 6)*

Prove sufficient completeness

We need to show that we can:

- S1 Determine correctness of well-formed expression e.
- S2 Decide the value of e, if e is correct query.

Prove sufficient compeleteness by structural induction

Base case: new_account is correct

balance (new_account (o)) is correct and value is 0

owner (new_account (o)) is correct and value is o

Step case: assume expression e with n nested level is correct, prove that we can decide whether e' with n+1 nested level:

- balance (e') is correct
- owner(e') is correct
- deposit (e', v) is correct
- withdraw (e', v) is correct

And in the first two cases when e' is correct and, show we can decide its value.

Prove sufficient compeleteness – Base case

Base case: to prove

- new_account is correct

Proof:

Because new_account has no precondition, so it is correct.

Prove sufficient compeleteness – Base case

Base case: to prove

- balance (new_account (o)) is correct and value is 0

Proof:

balance (new_account (o)) is correct because new_account(o) is correct and balance has no precondition.

Value of balance(new_account(o)) is 0 axiom1

Prove sufficient compeleteness – Base case

Base case: to prove

- owner (new_account (o)) is correct and value is o

Prove:

owner(new_account(o)) is correct because new_account(o) is correct and owner has no precondition.

Value of owner(new_account(o)) is o axiom2

Note that o itself can contain function of BANK_ACCOUNT

o = owner (deposit (new_account (“John”), 100))

Another structural induction needed here

Prove sufficient compeleteness – Step case

Assume expression e with n nested levels is correct and if the outermost function is query, value can be decided.

Prove that correctness of balance (e') can be decided, and show its value, where e' is with n+1 nested levels.

Proof:

e' can be of either form: deposit (e, v) or withdraw (e, v)

Case 1: e' is deposit (e, v)

balance(e') is balance (deposit (e, v)), it is correct iff v>=0.

When e' is correct, its value is:

balance (deposit (e, v)) = balance (e) + v axiom3

Case 2: e' is withdraw (e, v)

balance (e') is balance (withdraw (e, v)),

it is correct iff v>=0 and balance (e) >=v.

When e' is correct, its value is:

balance (withdraw (e, v)) = balance (e) – v axiom 4

Prove sufficient compeleteness – Step case

Assume expression e with n nested levels is correct and if expression, value can be decided.

Prove that correctness of owner (e') can be decided, and show its value, where e' is with n+1 nested levels.

Prove:

e' can be of either form: deposit (e, v) or withdraw (e, v)

Case 1: e' is deposit (e, v)

owner (e') is owner (deposit (e, v)), it is correct when e is correct and v>=0.

When e' is correct, its value is:

owner (deposit (e, v)) = owner (e) axiom5

Case 2: e' is withdraw (e, v)

owner (e') is owner (withdraw (e, v)),

it is correct when e is correct and v>=0 and balance (e) >=v.

When e' is correct, its value is:

owner (withdraw (e, v)) = owner (e) axiom 6

Prove sufficient compeleteness – Step case

Assume expression e with n nested levels is correct

Prove that correctness of e’ with n+1 nested level can be decided, where e’ is deposit (e, v)

Prove:

deposit (e, v) is correct iff e is correct and v>=0

Prove sufficient compeleteness – Step case

Assume expression e with n nested levels is correct

Prove that correctness of e’ with n+1 nested level can be decided, where e’ is withdraw (e, v)

Prove:

withdraw (e, v) is correct iff e is correct and v>=0 and balance (e) >= v

QED

Transfer money: ADT PAIR

TYPES

PAIR [G, H]

FUNCTIONS

new_pair: G x H → PAIR [G, H]

first: PAIR [G, H] → G

second: PAIR [G, H] → H

AXIOMS

first (new_pair (x, y)) = x

second (new_pair (x, y)) = y

Transfer money

FUNCTIONS

transfer: ACCOUNT × ACCOUNT × INTEGER → PAIR [ACCOUNT, ACCOUNT]

PRECONDITIONS (with v ∈ INTEGER, a, b ∈ ACCOUNT)

transfer (a, b, v) require balance (a) ≥ v and v ≥ 0

AXIOMS

transfer (a, b, v) = new_pair (withdraw (a, v), deposit (b, v))