Hyperproperties

Michael George

Stanford, August 2022

Comparing hypothetical executions

Often, we want to say that two operations have the same effects

- Two small deposits are the same as one big deposit
- Adding permissions doesn’t cause reverts
- Staking more earns more
- Staking longer earns more

CVL allows saving and restoring the state of the world

- `storage` type represents a snapshot of storage
- `lastStorage` gives the current state of storage
- `f(...) at s` resets the storage before executing `f`

certora

Example

- Want to show that transferring a and the b is the same as transferring a + b

```
//// certora/specs/ERC20.spec

/// transferring `a` tokens and then then `b` tokens has the same effect as
/// transferring `a+b` tokens
rule transferFromAdditive {
    address sender; address recipient;
    uint amount_a; uint amount_b;

    storage init = lastStorage;                                  // save storage

    transferFrom(sender, recipient, amount_a);
    transferFrom(sender, recipient, amount_b);

    mathint balance_sender_1 = balanceOf(sender);
    mathint balance_recip_1  = balanceOf(recipient);

    transferFrom(sender, recipient, amount_a + amount_b) at init; // restore storage

    mathint balance_sender_2    = balanceOf(sender);
    mathint balance_recipient_2 = balanceOf(recipient);

    assert balance_sender_1 == balance_sender_2,
        "two small transfers must change the sender's balance by the same amount as one large transfer";

    assert balance_recip_1 == balance_recip_2,
        "two small transfers must change the recipient's balance by the same amount as one large transfer";
}
```

certora