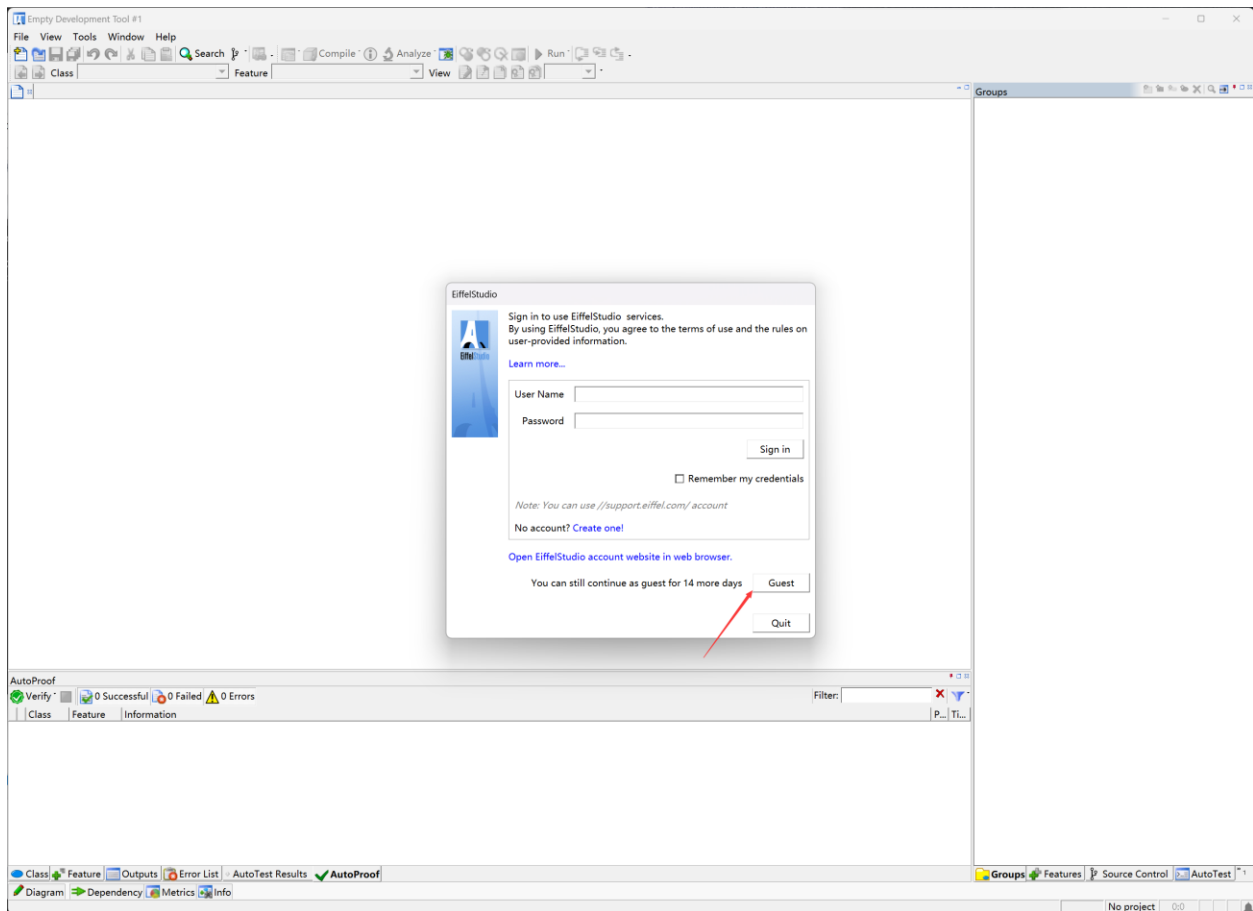


Example: Use Proof2Test for ACCOUNT example

1. Install EiffelStudio with AutoProof via <https://github.com/huangl223/ES-AP-Installation>

Follow the guidance in [./ES-AP-Installation/Install AutoProof on Windows.pdf](https://github.com/huangl223/ES-AP-Installation/blob/master/Install%20AutoProof%20on%20Windows.pdf)

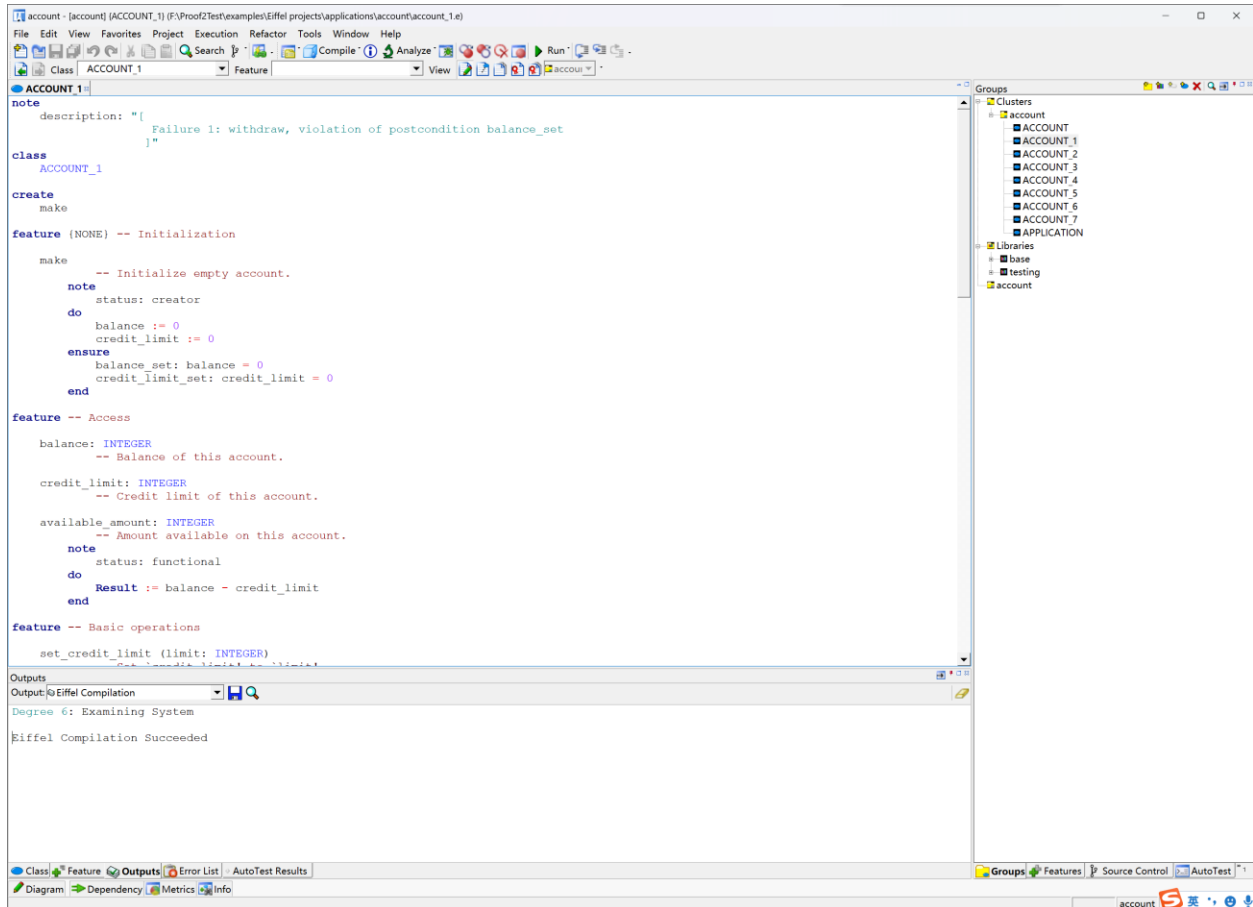
2. Launch EiffelStudio log in as Guest.



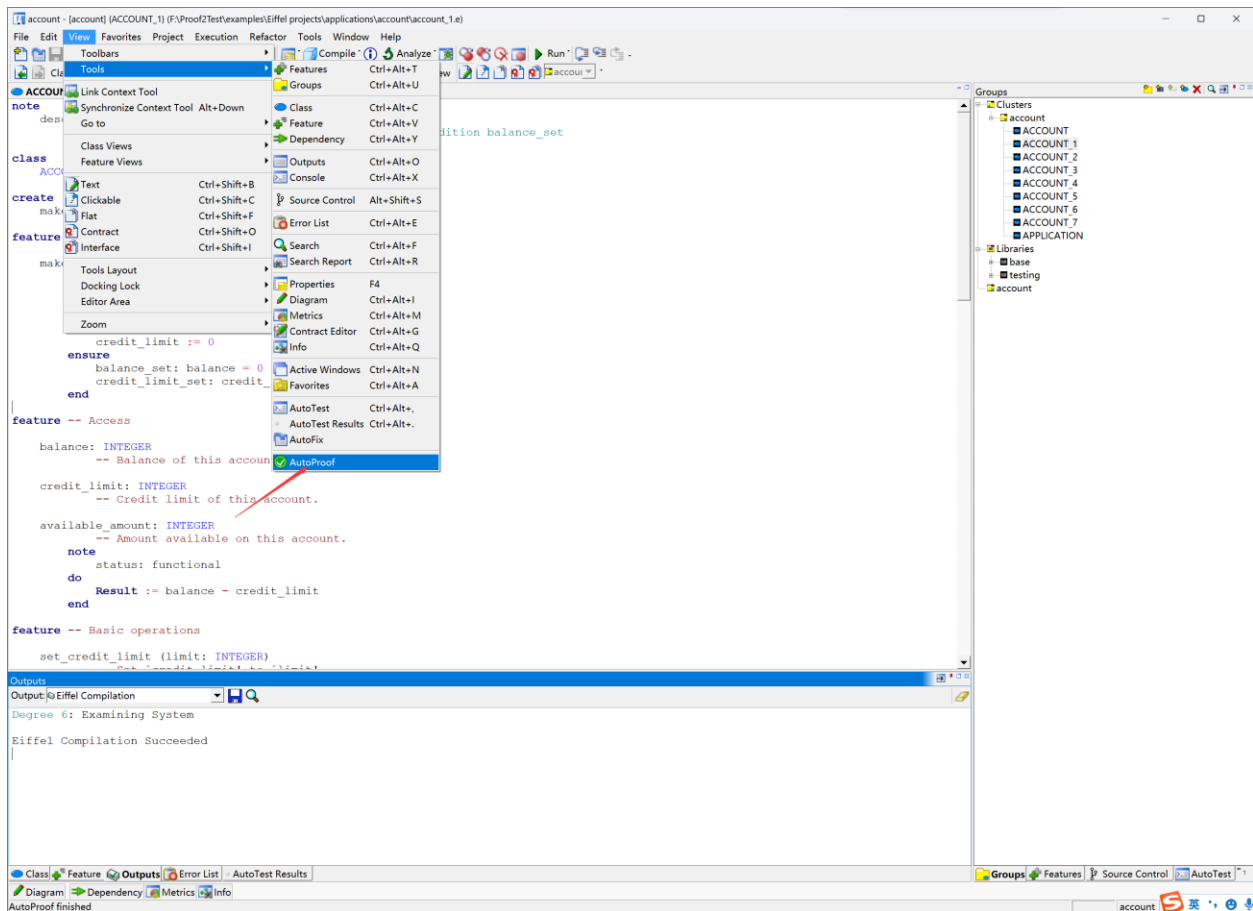
2. Open and compile the project

..\Proof2Test\examples\Eiffel projects\applications\account

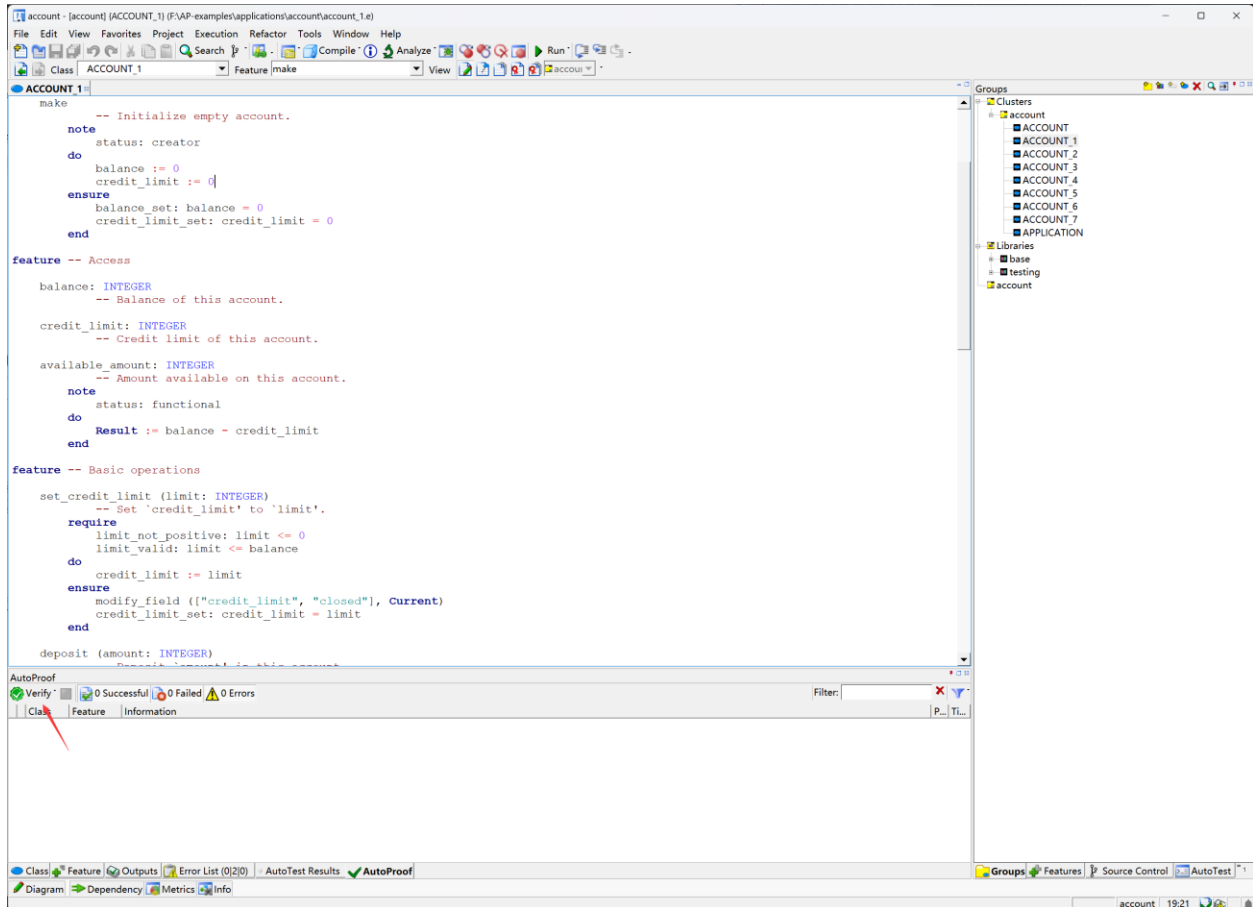
(select the account.ecf and open it)



3. Launch AutoProof tool panel via: View | Tools | AutoProof



4. Select ACCOUNT_1 class in the Group panel (righthand side); click Verify button in the AutoProof panel to start the verification.



account - [account] [ACCOUNT_1] (F:\VAP-examples\applications\account\account_1.e)

File Edit View Favorites Project Execution Refactor Tools Window Help

Class: ACCOUNT_1 Feature: set_credit_limit View: [Icons]

```
ACCOUNT_1
do
  balance := balance - amount
ensure
  modify_field(["balance", "closed"], Current)
  balance_set: balance = old balance + amount
  balance_decrease: balance <= old balance
end

transfer (amount: INTEGER; other: ACCOUNT_1)
  -- Transfer 'amount' from this account to 'other'.
note
  explicit: wrapping
require
  amount_not_negative: amount >= 0
  amount_available: amount <= available_amount
  other /= Current
do
  withdraw (amount)
  other.deposit (amount)
ensure
  modify_field(["balance", "closed"], [Current, other])
  withdrawal_made: balance = old balance - amount
  desposit_made: other.balance = old other.balance + amount
end

invariant
  credit_limit_not_positive: 0 >= credit_limit
  balance_non_negative: balance >= credit_limit

end
```

Groups

- Clusters
 - account
 - ACCOUNT
 - ACCOUNT_1
 - ACCOUNT_2
 - ACCOUNT_3
 - ACCOUNT_4
 - ACCOUNT_5
 - ACCOUNT_6
 - ACCOUNT_7
 - APPLICATION
- Libraries
 - base
 - testing
 - account

AutoProof

Verify [Icons] 0 Successful 0 Failed 0 Errors Filter: [X] [v]

Class Feature Information [P...] [T...]

Class Feature Outputs Error List (0/20) AutoTest Results AutoProof

Diagram Dependency Metrics Info

Boogie running: 0 s

account 52:13 [Icons]

account - [account] [ACCOUNT_1] (F:\VAP-examples\applications\account\account_1.e)

File Edit View Favorites Project Execution Refactor Tools Window Help

Class: ACCOUNT_1 Feature: set_credit_limit View: [Icons]

```
do
  balance := balance - amount
ensure
  modify_field(["balance", "closed"], Current)
  balance_set: balance = old balance + amount
  balance_decrease: balance <= old balance
end

transfer (amount: INTEGER; other: ACCOUNT_1)
  -- Transfer 'amount' from this account to 'other'.
note
  explicit: wrapping
require
  amount_not_negative: amount >= 0
  amount_available: amount <= available_amount
  other /= Current
do
  withdraw (amount)
  other.deposit (amount)
ensure
  modify_field(["balance", "closed"], [Current, other])
  withdrawal_made: balance = old balance - amount
  desposit_made: other.balance = old other.balance + amount
end

invariant
  credit_limit_not_positive: 0 >= credit_limit
  balance_non_negative: balance >= credit_limit

end
```

Groups

- Clusters
 - account
 - ACCOUNT
 - ACCOUNT_1
 - ACCOUNT_2
 - ACCOUNT_3
 - ACCOUNT_4
 - ACCOUNT_5
 - ACCOUNT_6
 - ACCOUNT_7
 - APPLICATION
- Libraries
 - base
 - testing
 - account

AutoProof

Verify [Icons] 6 Successful 1 Failed 0 Errors Filter: [X] [v]

| Class | Feature | Information | P... | T... |
|-----------|-------------------------|--|------|------|
| ACCOUNT_1 | invariant admissibility | Verification successful. | | 0.16 |
| ACCOUNT_1 | make (creator) | Verification successful. | | 0.00 |
| ACCOUNT_1 | available_amount | Verification successful. | | 0.04 |
| ACCOUNT_1 | set_credit_limit | Verification successful. | | 0.01 |
| ACCOUNT_1 | deposit | Verification successful. | | 0.00 |
| ACCOUNT_1 | withdraw | Postcondition balance_set may be violated. | 77 | 0.08 |
| ACCOUNT_1 | transfer | Verification successful. | | 0.02 |

Class Feature Outputs Error List (0/20) AutoTest Results AutoProof

Diagram Dependency Metrics Info

AutoProof finished

account 52:13 [Icons]




7. Add the directory of `proof2test.exe` to the values of the environment variable **PATH**

`..\Proof2Test\executable`

8. Go to the folder (where the .bpl and .model files locate)

`.. Proof2Test\examples\Eiffel projects\applications\account\EIFGENs\account\Proofs`

Proof2Test > examples > Eiffel projects > applications > account > EIFGENs > account > Proofs

| Name | Date modified | Type | Size |
|--|-------------------|------------|-------|
|  autoproof0.bpl | 4/11/2023 9:19 PM | BPL File | 65 KB |
|  ce0 | 4/11/2023 9:19 PM | MODEL File | 13 KB |
|  output0 | 4/11/2023 9:19 PM | 文本文档 | 2 KB |

9. Use Command Line interface and use the following Proof2Test command to generate test

`proof2test -b autoproof0.bpl -m ce0.model`

```
F:\Proof2Test\examples\Eiffel projects\applications\account\EIFGENs\account\Proofs>proof2test -b autoproof0.bpl -m ce0.model
Warning could not open Eiffel update file D
From directory F:\Proof2Test\examples\Eiffel projects\applications\account\EIFGENs\account\Proofs
Error 2: No such file or directory
Output test file: new_test_set.e
F:\Proof2Test\examples\Eiffel projects\applications\account\EIFGENs\account\Proofs> |
```

10. Go back to the EiffelStudio IDE, go to the Group Panel, create a class named `NEW_TEST_SET`, under the `account` cluster.

account - [account] (ACCOUNT) (C:\Users\HP\Documents\GitHub\Proof2Test\examples\Eiffel\projects\applications\account\account.e)

File Edit View Favorites Project Execution Refactor Tools Window Help

Class ACCOUNT Feature View Compile Analyze Run

```
1 note
2   explicit: "all"
3
4 class
5   ACCOUNT
6
7 create
8   make
9
10 feature {NONE} -- Initialization
11
12   make
13     -- Initialize empty account.
14
15   note
16     status: creator
17
18   do
19     balance := 0
20     credit_limit := 0
21   ensure
22     balance_set: balance = 0
23     credit_limit_set: credit_limit
24   end
25
26 feature -- Access
27
28   balance: INTEGER
29     -- Balance of this account.
30
31   credit_limit: INTEGER
32     -- Credit limit of this account
33
34   available_amount: INTEGER
```

Add New Class

Identification

Class name: NEW_TEST_SET

Cluster:

- account
 - ACCOUNT
 - ACCOUNT_1
 - ACCOUNT_2
 - ACCOUNT_3
 - ACCOUNT_4
 - ACCOUNT_5
 - ACCOUNT_6

General

☐ deferred ☐ expanded

☐ Generate creation procedure make

☐ Generate default feature clauses

Parents:

Add... Remove

Create Cancel

Groups

- Clusters
 - account
 - ACCOUNT
 - ACCOUNT_1
 - ACCOUNT_2
 - ACCOUNT_3
 - ACCOUNT_4
 - ACCOUNT_5
 - ACCOUNT_6
 - ACCOUNT_7
 - APPLICATION
- Libraries
 - base
 - testing
 - account

AutoProof

Verify 6 Successful 1 Failed 0 Errors

| Class | Feature | Information | P... | Ti... |
|----------|----------------|--|------|-------|
| ACCOU... | invariant a... | Verification successful. | | 0.58 |
| ACCOU... | make (cre... | Verification successful. | | 0.01 |
| ACCOU... | available... | Verification successful. | | 0.03 |
| ACCOU... | set_credit... | Verification successful. | | 0.02 |
| ACCOU... | deposit | Verification successful. | | 0.00 |
| ACCOU... | withdraw | Postcondition balance_set may be violated. | 77 | 0.04 |
| ACCOU... | transfer | Verification successful. | | 0.01 |

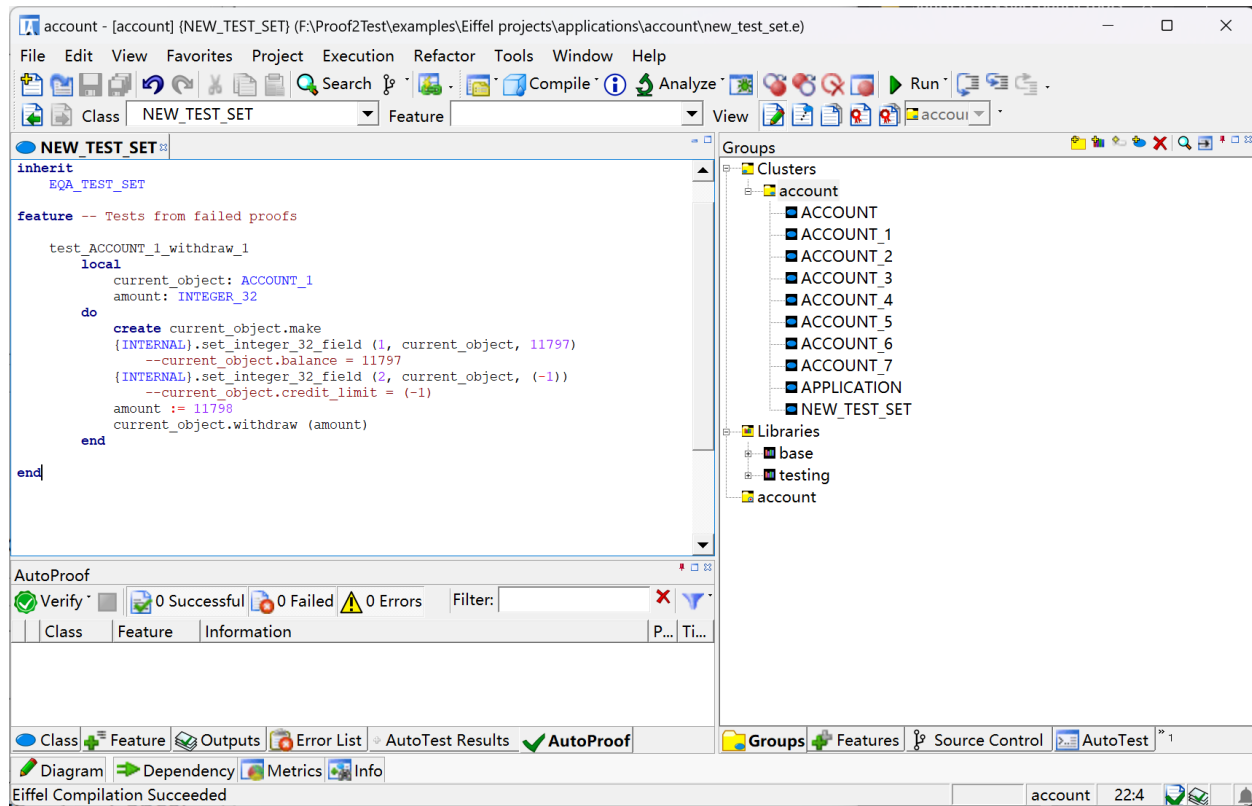
Class Feature Outputs Error List (0/73/0) AutoTest Results AutoProof

Diagram Dependency Metrics Info

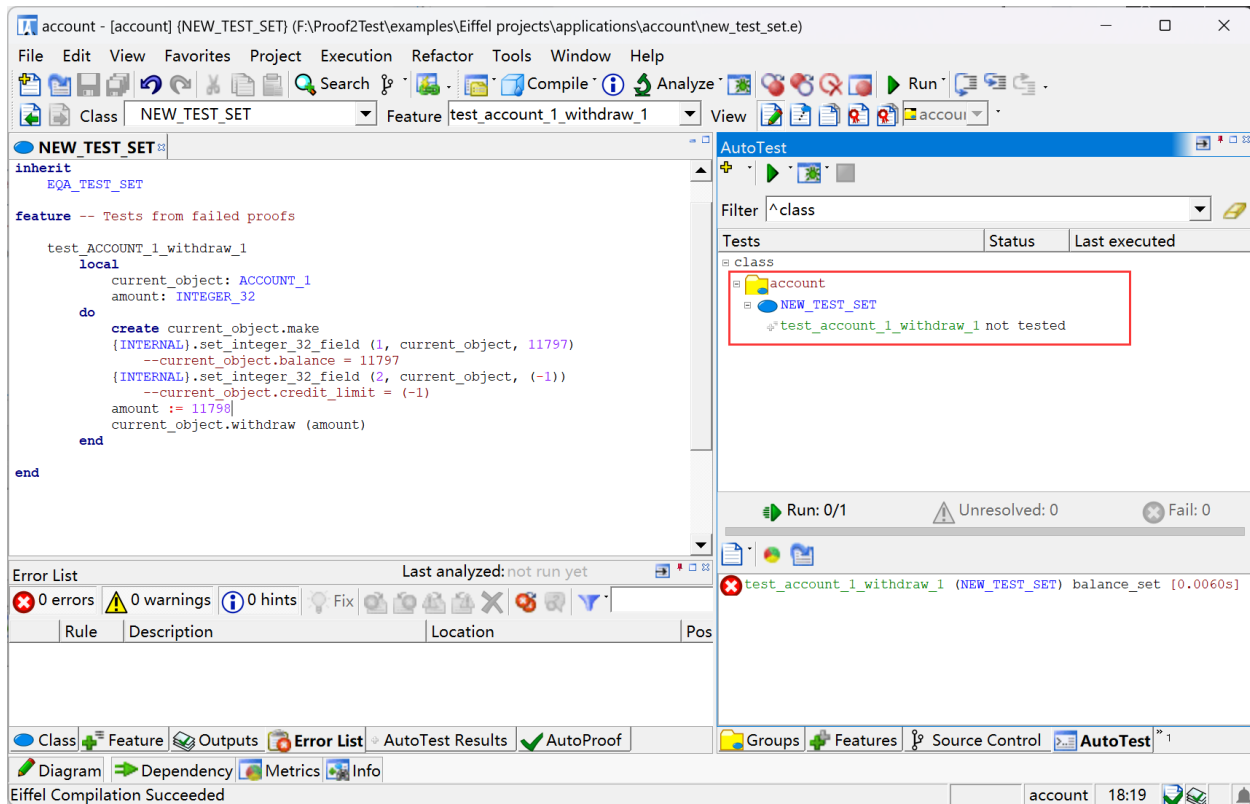
Groups Features Source Control AutoTest



account 1:1

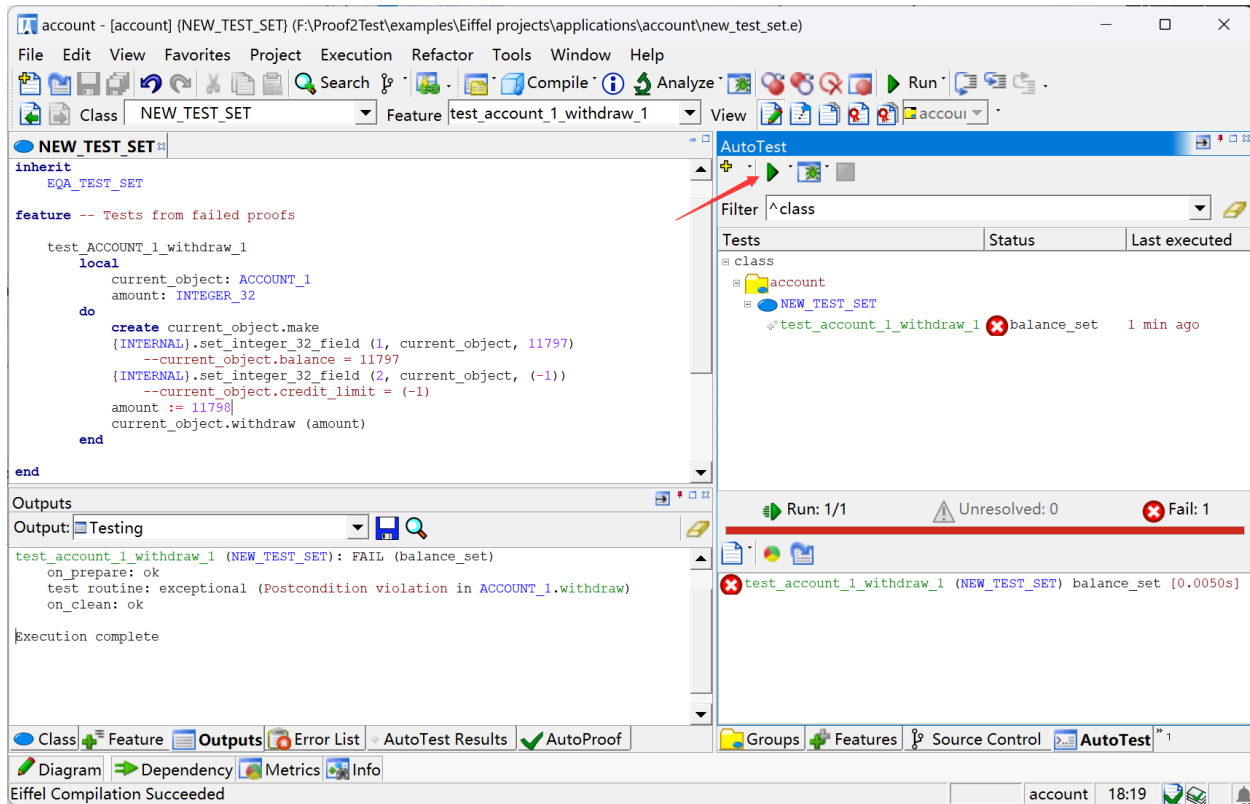
11. Copy-paste the content of the [new_test_set.e](#) into the class; and compile the project.



12. After compilation finishes, go to the AutoTest panel (the last tab in the righthand side); and you will see the test case is listed in the panel.



13. At this point, you can click the Run button  to run the test case; or click the Debug button  to switch to the debug mode and inspect the program behaviors step by step.



account - [account] {NEW_TEST_SET} (F:\Proof2Test\examples\Eiffel projects\applications\account\new_test_set.e)

File Edit View Favorites Project Execution Refactor Tools Window Help

Class NEW_TEST_SET Feature test_account_1_withdraw_1 View

NEW_TEST_SET

```
inherit
  EQA_TEST_SET

feature -- Tests from failed proofs

  test_ACCOUNT_1_withdraw_1
    local
      current_object: ACCOUNT_1
      amount: INTEGER_32
    do

```

AutoTest Results

Details Comparison

bn_prepare: ok
test routine: exceptional (Postcondition violation in ACCOUNT_1.withdraw)

***** Thread exception *****
In thread Root thread 0x0 (thread id)

| Class / Object | Routine | Nature of exception | Effect |
|------------------------------------|------------------------------|---|--------|
| ACCOUNT_1 <00000233C462CF58> | withdraw @5 | balance_set: Postcondition violated. | Fail |
| ACCOUNT_1 <00000233C462CF58> | withdraw @5 | Routine failure. | Fail |
| NEW_TEST_SET <00000233C462B0D8> | test_account_1_withdraw_1 @5 | Routine failure. | Fail |

on_clean: ok

AutoTest

Filter ^class

| Tests | Status | Last executed |
|---------------------------|-------------|---------------|
| class | | |
| account | | |
| NEW_TEST_SET | | |
| test_account_1_withdraw_1 | balance_set | 1 min ago |

Run: 1/1 Unresolved: 0 Fail: 1

test_account_1_withdraw_1 (NEW_TEST_SET) balance_set [0.0050s]

Class Feature Outputs Error List AutoTest Results AutoProof Groups Features Source Control AutoTest

Diagram Dependency Metrics Info

Eiffel Compilation Succeeded

account 18:19