Formal Verification
- Coffee Vending Machine

2009.12.18

Team 3. 원승호, 최성은, 조승철
Database Lab. In Konkuk Univ.

Description (1/1)

- Coffee, Milk, KoreanTea 3가지 종류를 판매 한다
  - Coffee – 200원 Milk – 300원 KoreanTea – 400원
- 10, 50, 100, 500, 1000원의 형태로 투입 가능하다.
- 자판기는 음료선택 과 반환 버튼을 가지고 있다.
- 음료는 동시에 2개가 나올 수 없다
- 금액은 5000원 이상이 될 수 없다.
- 금액이 200원 이상이 되면 구입 가능 하다.

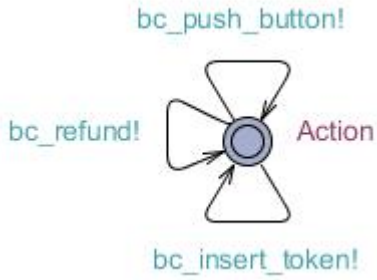
Description (2/2)

❖ 돈 투입 후 5초 이내에 음료를 선택하지 않으면 돈을 반환 한다.

❖ 음료 선택 후 5초 내에 나와야 한다.

Timed Automata (1/6)

❖ Customer

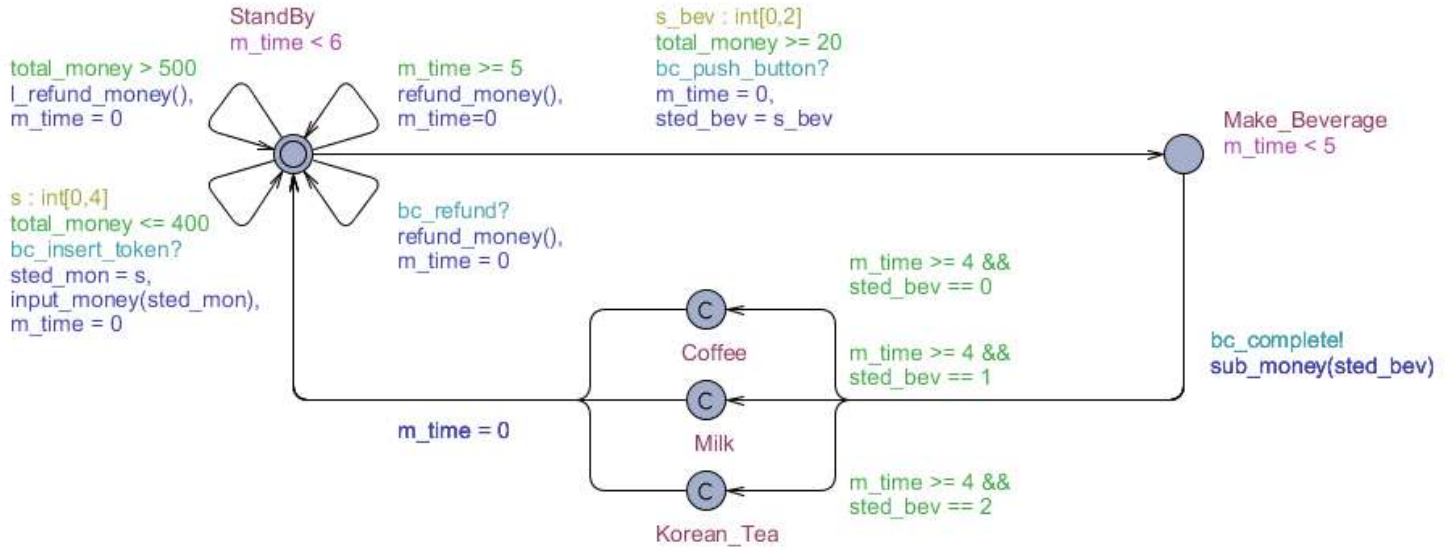


❖ State
- ◆ Action

❖ 보내는 Message
- ◆ bc_insert_token, bc_push_button, bc_refund

Timed Automata (2/6)

❖ CVM



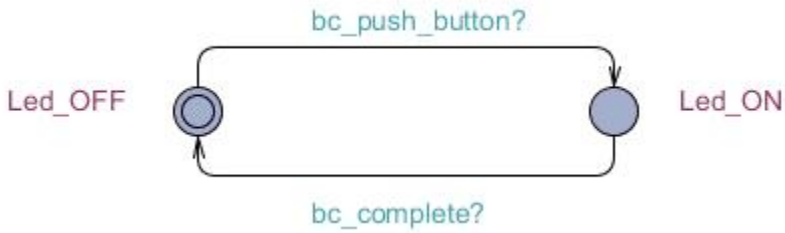
❖ State

- StandBy, Make_Beverage, Coffee (Milk, Korean_Tea)

Timed Automata (3/6)

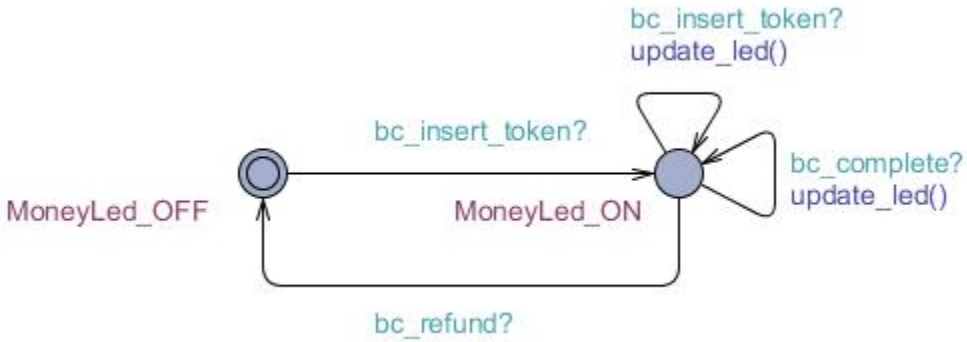
- 받는 Message
  - bc_insert_token, bc_refund, bc_push_button
- 보내는 Message
  - bc_complete

Timed Automata (4/6)



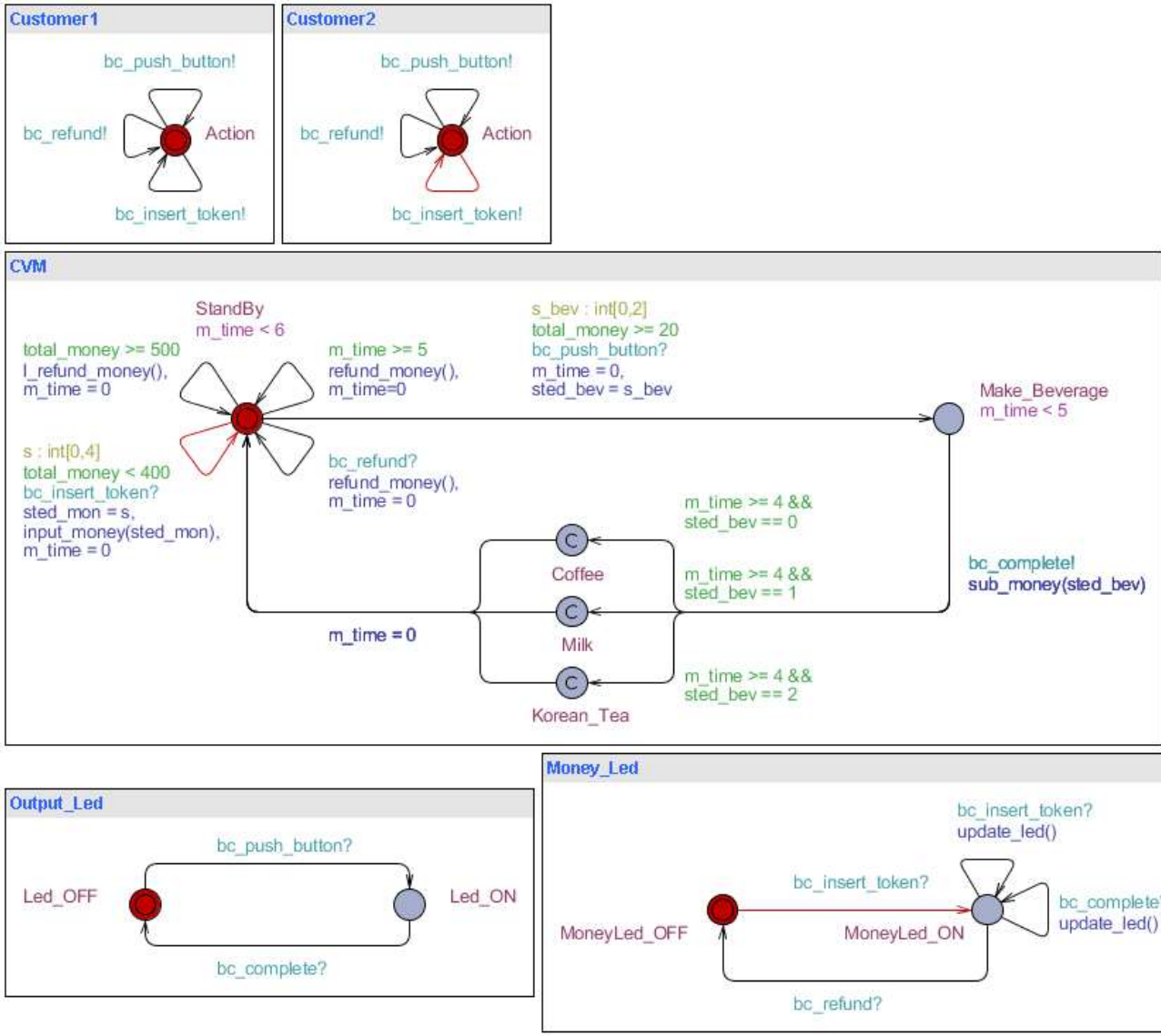
- State
  - Led_OFF, Led_ON
- 받는 Message
  - bc_push_button, bc_complete

Timed Automata (5/6)



- State
  - MoneyLed_OFF, MoneyLed_ON
- 받는 Message
  - bc_insert_button, bc_complete, bc_refund

Timed Automata (6/6)



Verification (1/4)

1. 모든 Path에서 모든 State는 데드락에 걸리지 않는다.
   - A[] not deadlock

2. 최대금액은 5000원 이상일 수 없다.
   - A[] not CVM.total_money > 500

3. 잔돈이 5000원 이상이면 그이상은 반환된다.
   - A[] CVM.total_money>500 imply CVM.l_refund_money()

4. 총 금액이 200원이상일때 음료를 선택할 수 있다 .
   (200원 이하일때 버튼 누르면 자판기는 무시함)
   - A[] CVM.Make_Beverage imply CVM.total_money >=20

Verification (2/4)

5. 음료가 나오면 전체 금액에서 음료 값을 빼준다.
   - A[] ((CVM.Coffee imply CVM.total_money-20) or (CVM.Milk imply CVM.total_money-30) or (CVM.Korean_Tea imply CVM.total_money-40))

6. 음료는 동시에 2개가 나올 수 없다.
   - A[] not (CVM.Coffee and CVM.Milk and CVM.Korean_Tea)

7. 자판기는 5초이내료 버튼을 누르지 않으면 반환을 한다
   - A[] (CVM.StandBy && m_time > 5) imply CVM.refund_money()

8. 음료는 5초이내로 나오고 선택한 음료가 나와야 한다
   - A[] (CVM.Coffee imply (m_time>=4 && CVM.sted_bev == 0)) && (CVM.Milk imply (m_time>=4 && CVM.sted_bev == 1)) && (CVM.Korean_Tea imply (m_time>=4 && CVM.sted_bev == 2))

Verification (3/4)

9. 음료를 선택되면 배출구 LED가 켜진다.
   - A[] CVM.Make_Beverage imply Output_Led.Led_ON

10. 10. 음료가 다 나오면 배출구 Led는 꺼진다.
   - A[] CVM.Coffee imply Output_Led.Led_OFF

11. 음료가 나오면 금액 Led를 업데이트 한다
   - A[] (CVM.Coffee or CVM.Milk or CVM.Korean_Tea) imply Money_Led.update_led()

12. 추가로 금액이 투입되면 금액Led를 업데이트 해준다
   - A[] Money_Led.MoneyLed_ON imply Money_Led.update_led()

Verification (4/4)

13. 금액을 투입하면 금액Led를 On 한다

- Money_Led.MoneyLed_OFF --> Money_Led.MoneyLed_ON
  imply CVM.input_money(CVM.sted_mon)

14. 14. 반환을 하면 금액Led를 Off 한다

- Money_Led.MoneyLed_ON --> Money_Led.MoneyLed_OFF
  imply CVM.refund_money()

사랑과 정성으로…

Thank You!!