Formal Verification of a Market Making Algorithm

By KangHyuk Lee and Arjun Somekawa

Background and Motivation

“It took only one defect in a trading algorithm for Knight Capital to lose $440 million in about 30 minutes. That $440 million is three times the company’s annual earnings.” [1]

What is a Market Maker?

Goal: provide liquidity to the market

Bid: highest price buyer willing to pay

Ask: lowest price a seller willing to accept

Spread: Ask - Bid

Mid-price: (Bid + Ask) / 2

Tools and Goals

PRISM
model checker

Our Atomic Propositions

1. Mid
2. Inventory
3. Bid
4. Max Limit
5. Ask
6. MarketDataRecieved
7. QuotePosted
8. CancelSent
9. OrderLive
10. Filled
11. Cancel Confirmed

Safety Properties

AG (bid < ask) : If bid is greater than the ask, it means that the algorithm is willing to buy a security and sell it for less than the amount it paid for it, which would lead to arbitrage loss as investors would take advantage by continuously selling the security and buying for a lower price.

AG (inventory < max limit) : The inventory should not hold more than a certain number of positions for each security to limit risk.

Liveness Properties

AG (market data received → AF (quote posted)) : When new market data is received, the algorithm should eventually post new bid/ask quotes.

AG (cancel sent → AF (filled v cancel confirmed)) : If a cancel request is sent out, either the order should get filled before cancellation or receive a cancel confirmation.

Using nuXml in our Project

```
nuXmv > go
nuXmv > check_ctlspec
-- specification AG bid < ask  is true
-- specification AG (marketDataReceived -> AF quotePosted)  is true
-- specification AG ((cancelSent & orderLive) -> AF (filled | cancelConfirmed))  is true
-- specification AG inventory <= maxLimit  is true
nuXmv > quit
```

PRISM

Probabilistic Symbolic Model Checker

Various models: DTMC, CTMC, MDP, PTA

MDP (Markov Decision Process): probabilistic + nondeterministic (choices)

Symbolic state space (BDD)

PCTL: probabilistic CTL

Rewritten properties

Safety

P>=1 [G (bid < ask)]

P>=1 [G (inv <= MAX_LIMIT & inv >= -MAX_LIMIT)]

Liveness

P>=1 [G (!pending_quote)]

P>=1 [G (!pending_cancel)]

Safety Property Results: P>=1 [G (bid < ask)]

```
Model checking: P>=1 [ G (bid<ask) ]

Building model (engine:symbolic)...

Computing reachable states...

Reachability (BFS): 40007 iterations in 7.58 seconds (average 0.000189, setup 0.00)

Time for model construction: 23.718 seconds.

Type:        MDP
States:      100010 (1 initial)
Transitions: 230021

Transition matrix: 756 nodes (3 terminal), 230021 minterms, vars: 46r/46c/4nd

Probability bound in formula is 0/1 so not computing exact probabilities...

yes = 0, no = 100010, maybe = 0

Property satisfied in 1 of 1 initial states.

Time for model checking: 0.004 seconds.

Result: true
```

Safety Property Results: P>=1 [G (inv <= MAX_LIMIT & inv >= -MAX_LIMIT)]

```
Model checking: P>=1 [ G (inv<=MAX_LIMIT&inv>=-MAX_LIMIT) ]

Probability bound in formula is 0/1 so not computing exact probabilities.

Prob0A: 4005 iterations in 0.45 seconds (average 0.000113, setup 0.00)

Prob1E: 4006 iterations in 0.61 seconds (average 0.000152, setup 0.00)

yes = 100010, no = 0, maybe = 0

Property satisfied in 0 of 1 initial states.

Time for model checking: 1.155 seconds.

Result: false
```

Prob0A: states from which property cannot be guaranteed
Prob1E: states from which property can potentially be guaranteed

Liveness Property Results: P>=1 [G (!pending_quote)]

```
Type:        MDP
States:      100010 (1 initial)
Transitions: 230021

Transition matrix: 756 nodes (3 terminal), 230021 minterms, vars: 46r/46c/4nd

Probability bound in formula is 0/1 so not computing exact probabilities...

Prob0A: 2 iterations in 0.00 seconds (average 0.000000, setup 0.00)

Prob1E: 3 iterations in 0.00 seconds (average 0.000000, setup 0.00)

yes = 100010, no = 0, maybe = 0

Property satisfied in 0 of 1 initial states.

Time for model checking: 0.003 seconds.

Result: false
```

Liveness Property Results: P>=1 [G (!pending_cancel)]

```
Model checking: P>=1 [ G (!pending_cancel) ]

Probability bound in formula is 0/1 so not computing exact probabilities.

Prob0A: 4 iterations in 0.00 seconds (average 0.000000, setup 0.00)

Prob1E: 5 iterations in 0.00 seconds (average 0.000000, setup 0.00)

yes = 100010, no = 0, maybe = 0

Property satisfied in 0 of 1 initial states.

Time for model checking: 0.002 seconds.

Result: false
```

Limitations

1) Symbolic: unable to test code directly
2) Unable to directly express G (p → F q): use auxiliary obligation variables (pending_quote and pending_cancel) instead
3) Local safety != global safety: a property could be true in every state but may still be deemed unsafe if not guaranteed forever
4) Counterexamples limited to DTMC (Discrete-Time Markov Chain) model

References

1. https://theluxuryplaybook.com/what-is-bid-ask-spread-how-it-works-in-trading/
2. https://www.prismmodelchecker.org/