Towards Formally Verified Finance with Linear Temporal Logic

A financial contract is a component in a reactive system

Quinn Dougherty

Casper Association - R&D

2024 Jan 17

* Logic
  → Introduction
  → Why it matters in financial software
* Linear Temporal Logic (LTL)
  → Beyond truth to truth *when*
* ACTUS
  → PAM in LTL
* LTL-ACTUS (demo)
  → A formal verification strategy for finance

Logic

» Logic

* What is logic
* Why it matters in financial software

» What is logic

Study of an argument's *structure*

Example: modus ponens

If it is raining, then the ground is wet. It is raining. Therefore, the ground is wet.

Example: modus tollens

If it is snowing, then it is cold outside. It is not cold outside. Therefore, it is not snowing.

» The connectives

And

$P \wedge Q$ if and only if P is true and Q is true.

Or

$P \vee Q$ if and only if at least one of P or Q is true

Not

$\neg$ if and only if P is not true

» The quantifiers

For all / for every

$\forall x, Px$ is true if P is always true regardless of what x is

There exists / for some

$\exists x, Px$ is true if P is true at least once throughout values of x

» Why logic matters in software and finance

Beyond quality assurance

Testing on steroids: quantified proofs rather than piecemeal instances

Formal verification

* Quantify (“for all”) over a program’s inputs, execution traces of nondeterministic programs, or over all programs of a language
* Prove correctness with respect to a specification

Linear Temporal Logic (LTL)

» Linear Temporal Logic (LTL)

* Beyond truth to truth *when*
* Logic that's aware of timestep

» The modal operators

Always

$\Box P$ is true if P is true regardless of timestep

Eventually

$\Diamond P$ is true if P will come true at some timestep, but possibly not yet

» Verifying a traffic light with LTL

A traffic light should never be green in all directions

$$\Box\left((\text{northGreen} \wedge \text{southGreen}) \rightarrow \neg(\text{eastGreen} \vee \text{westGreen})\right)$$

A traffic light should eventually turn green in all directions

$$\Box\Diamond\text{northGreen} \wedge \Box\Diamond\text{southGreen} \wedge \Box\Diamond\text{eastGreen} \wedge \Box\Diamond\text{westGreen}$$

Algorithmic Contract Types Unified Standard (ACTUS)

» PAM

Pay interest periodically, but principal only at end of term

» PAM in LTL

The terms are static throughout lifetime of contract

$\square$ Terms(`principal`=1000, `ir`=0.05, `months`=24)

The eventual total repayment is equal to the principal plus interest

$\Diamond$ State(`total_repayment`=`principal` * (1 + `ir` / 12) * `months`)

We connect each of these temporal propositions together with "and" ($\wedge$)

LTL-ACTUS (demo)

» LTL-ACTUS (demo)

Linear temporal logic as the financial execution environment

» Demo