What Criminal and civil law tells about Safe RL techniques to generate Law-abiding behaviour

SafeAI at AAAI 2021

Hal Ashton

Almost every environment is regulated by law

In the event of harm being caused by an autonomous algorithmic agent, someone will be on the hook.

Social or Economic pressures mean that eventually responsibility will come back to the programmer.

Lots of different kinds of laws exist.

The Paper positions itself in Safe Reinforcement Learning literature, but conclusions are relevant across any learning technique.

Lots of different kind of laws exist

Distinguish between States -measurable attributes of the world lasting a certain amount of time.

And Actions - things that an autonomous can choose to do which may change the state of the world.

A simple non-exhaustive list of law types:

1. Don't reach this state.
2. Don't act (behave) like that.
3. Don't cause this state.
4. Don't intend to do that.
5. And any mix of the above: Don't act like this to intend to cause that state.

*Offences also possible through omission, so 'Don't' also replaceable by 'Do'!
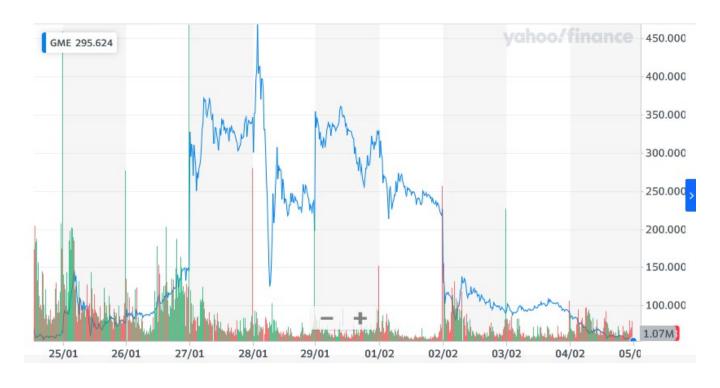
A Topical example – GameStop!

Private investors, coordinated through Reddit to buy stock in GameStop, a US listed stock.

The stock had been heavily shorted by Hedge funds.

Through coordinated buying, the Private investors aimed to create a short-squeeze.

A short squeeze is where a large upward price move causes short-sellers to buy stock to close their position.

The additional buying further reduces supply which further raises prices.

A Topical example – Don't `act` like this to `intend` to `cause` that.

This is an example of **market manipulation**. It is prohibited in almost every market worldwide.

It can be both a civil and criminal offence.

Logically, if you buy a stock it is because you believe the stock price will rise.

Crucially, you must believe it will rise not as a result of you buying. (But-for causality).

Most market manipulation attempts are unsuccessful and fail eventually.

Hence intention to alter the price of a stock through trading is also an offence.

A Topical example -Don't `act` like this to `intend` to `cause` that.

Algorithms account for the majority of transactions in nearly every exchange traded market.

With a limited action set, structured data sets and huge potential rewards.

Algorithmic trading is an attractive area to deploy machine learning.

Market manipulation can be a profitable strategy.

Algorithms are subject to the same laws as any other exchange participant.

So how do you train a trading algorithm to be good at its job and not to manipulate markets?

Thanks

- ucabha5@ucl.ac.uk
- Twitter: @hal_ashton