Introduction to

QUANTUM MODEL CHECKING

FRANCESCO TESTA
1179083

Model Checking

- *"how can I be sure my system works as expected ?"*
- Different strategies: Model Checking, Abstract Interpretation, ...
- Model Checking is widely used:
  - we can be sure that the system fulfills all checked properties.
  - otherwise, it is usually possible to **provide a counterexample**, trace the source of the bug and fix it.

- Based on the presence or the absence of these aspects:
  - **probabilistic** behavior,
  - **non-deterministic** behavior
  - amount of **time available** to complete tasks,
- different models and model checking algorithms have been developed.

Quantum Model Checking

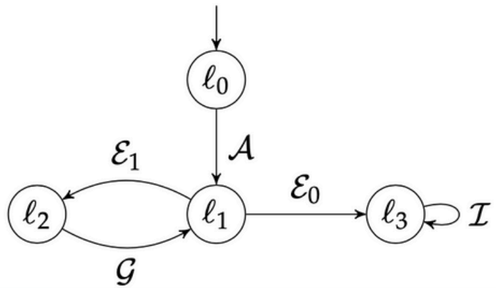
- Can be used to verify **quantum protocols**, like quantum key distribution.
- Quantum mechanics is not intuitive, due to quantum phenomena like entanglement or superposition.
- It's easier to unintentionally **introduce bugs** in protocols.
- Erroneous protocols can have a large impact on the usability and reliability of quantum systems.
- In order to apply model checking to quantum protocols, we need to answer two questions:
  1. How can we **model formally** the given quantum protocol?
  2. How can we **specify** the desired **properties**?

Model quantum procotol

- Quantum system is continuous. The state space is represented as a *d*-dimensional Hilbert Space $\mathscr{H}_d$.
- Model checking usually expects to deal with finite state spaces, so depending on the formula to be analyzed, the continuous behavior is first made discrete.
- Use of **Quantum Markov Chain**:
  - classical, discrete state space of Markov Chain,
  - replacing of the classic probability values decorating the transitions with **super-operators:** linear operator that acts on the space of linear operators.

Example

ℓ_0: $q := \mathcal{A}(q)$;
ℓ_1: **while** $M[q]$ **do**
ℓ_2: $q := \mathcal{G}(q)$;
ℓ_3: **end**



$$A = \{E_0, E_1\}$$

$$E_0 = |0\rangle\langle 0| + \frac{1}{\sqrt{2}}|1\rangle\langle 1|, E_1 = \frac{1}{\sqrt{2}}|0\rangle\langle 1|$$

$$M = \lambda_0|0\rangle\langle 0| + \lambda_1|1\rangle\langle 1|$$

$$\mathcal{E}_0 = \{|0\rangle\langle 0|\} \quad \mathcal{E}_1 = \{|1\rangle\langle 1|\}$$

- Classical states correspond to single steps of the quantum system
- Transitions are decorated with the **components** of the super-operators

Specify properties

- Computation Tree Logic (**CTL**)
  - focuses on the possible future behaviors of a system
  - considers *all* possible successor
- Fidelity Computation Tree Logic (**FCTL**)
  - introduction of *fidelity operator* to quantify similarity between quantum states
- Linear-time Temporal Logic (**LTL**)
  - focuses on a single execution of the system
  - can be extended to check ω- regular properties

Quantum Markov Chain

A super-operator weighted Markov chain $\mathfrak{M}$ over a Hilbert space $\mathcal{H}$ is a pair $\mathfrak{M} = (S, Q)$ where:

- S is a *finite state* of classical states;
- $Q : S \times S \to \mathcal{S}^{\mathcal{I}}(H)$ is called *transition matrix* where $\forall s \in S, \sum_{s' \in S} Q(s, s') \eqsim \mathcal{I}_{\mathcal{H}},$ that is *trace-preserving*.

- The **trace** denotes the probability that this specific evolution has occurred:
  - we write $\mathcal{E} \lesssim \mathcal{F}$ if $tr(\mathcal{E}(\rho)) \leq tr(\mathcal{F}(\rho))$
- $\mathcal{S}^{\mathcal{I}}(H)$ represents the counterpart of the probability domain [0,1]:

$$\mathcal{S}^{\mathcal{I}}(H) = \{\mathcal{E} \in \mathcal{S}(H) | 0_{\mathcal{H}} \lesssim \mathcal{E} \lesssim \mathcal{I}_{\mathcal{H}}\}$$

$$\mathcal{E} \in \mathcal{S}^{\mathcal{I}}(\mathcal{H}) \iff tr(\mathcal{E}(\rho)) \in [0, 1]$$

Quantum Markov Chain

It is needed the introduction of a measurable space. It will be based on the notion of **Path.**

- Given a QMC $\mathfrak{M} = (S, Q)$, a path is a finite or infinite sequence $\sigma = s_0, s_1, \ldots$ in $\mathfrak{M}$ if $\forall i \geq 1, Q(s_{i-1}, s_i) \neq 0_{\mathcal{H}}$
- We denote $\mathrm{Path}^{\mathfrak{M}}$ the set of infinite path, $\mathrm{Path}^{\mathfrak{M}}_{fin}$ the set of finite path and $\sigma[i]$ the state s_i
- The basic events of measurable space starting from a path σ : a set containing all possible infinite paths that are extension of σ .
- The measurable space is $(\mathrm{Path}^{\mathfrak{M}}, \Sigma)$, where Σ represents all measurable events.

$$Q^{\mathfrak{M}}_s(s_0 s_1 \cdots s_n) = \begin{cases} \mathcal{O}_{\mathcal{H}} & \text{if } s_0 \neq s; \\ \mathcal{I}_{\mathcal{H}} & \text{if } s_0 = s \text{ and } n = 0; \\ \mathbf{Q}(s_{n-1}, s_n)\mathbf{Q}(s_{n-2}, s_{n-1}) \cdots \mathbf{Q}(s_0, s_1) & \text{if } s_0 = s \text{ and } n > 0. \end{cases}$$

Labelled QMC

A labelled quantum Markov chain (LQMC) is a tuple $\mathfrak{M} = (S, \mathbf{Q}, AP, L)$ where $(S, \mathbf{Q})$ is a QMC and:

- AP is a *finite set* of atomic propositions;
- $L : S \to 2^{AP}$ is a labelling function

QCTL

Classical CTL	**Quantum CTL**
State formulas and **Path** formulas	**State** formulas and **Path** formulas
Use of $\forall$ and $\exists$ to quantify path formulas	Use of a single quantum quantifier, which accumulates the super-operators corresponding to the paths satisfying the given path formula and compares it with $\mathcal{E}$ $\mathbb{Q}_{\sim\mathcal{E}}$

QCTL

$$\varphi ::= a \mid \varphi \wedge \varphi \mid \neg\varphi \mid \mathbb{Q}_{\sim\mathcal{E}}[\psi]$$
$$\psi ::= \mathbf{X}\varphi \mid \varphi\,\mathbf{U}_{\leq k}\,\varphi \mid \varphi\,\mathbf{U}\,\varphi$$

$s \models a$	if $a \in L(s)$;
$s \models \varphi_1 \wedge \varphi_2$	if $s \models \varphi_1$ and $s \models \varphi_2$;
$s \models \neg\varphi$	if it is not the case that $s \models \varphi$;
$s \models \mathbb{Q}_{\sim\mathcal{E}}[\psi]$	if $Q_s^{\mathfrak{M}}(\{\sigma \in \mathrm{Path}^{\mathfrak{M}} \mid \sigma \models \psi\}) \sim \mathcal{E}$.

$\sigma \models \mathbf{X}\varphi$	if $\sigma[1] \models \varphi$;
$\sigma \models \varphi_1 \mathbf{U}_{\leq k} \varphi_2$	if $\exists n : 0 \leq n \leq k : \sigma[n] \models \varphi_2$ and $\forall i < n : \sigma[i] \models \varphi_1$;
$\sigma \models \varphi_1 \mathbf{U} \varphi_2$	if $\exists n \in \mathbb{N} : \sigma[n] \models \varphi_2$ and $\forall i < n : \sigma[i] \models \varphi_1$.

Let $\mathcal{M}$ be an LQMC, $s \in \mathcal{S}$ be a state, and φ be a QCTL state formula.
The model checking problem for $\mathcal{M}$ against φ asks to verify whether $s \models \varphi$ holds.

QCTL

To check if a LMQC satisfies a formula, the **standard bottom-up** approach will be used: given a state formula, it's computed the set of state satisfying the subformula (for each subformula).

Let's denote the set of state satisfying a state formula:

$$Sat(\phi) = \{s \in S | s \vDash \phi\}$$

This set is computed recursively:

$$\begin{aligned}
\mathrm{Sat}(a) &= \{s \in S \mid a \in L(s)\} \\
\mathrm{Sat}(\varphi_1 \wedge \varphi_2) &= \mathrm{Sat}(\varphi_1) \cap \mathrm{Sat}(\varphi_2) \\
\mathrm{Sat}(\neg\varphi) &= S \setminus \mathrm{Sat}(\varphi) \\
\mathrm{Sat}(\mathbb{Q}_{\sim\mathcal{E}}[\psi]) &= \{s \in S \mid Q_s^{\mathfrak{M}}(\{\sigma \in \mathrm{Path}^{\mathfrak{M}} \mid \sigma \models \psi\}) \sim \mathcal{E}\}
\end{aligned}$$

QCTL

The computation of $Q_s^{\mathfrak{M}}$ depends on the actual path formula that need to be satisfied

- **Next** operator (***X***)*:*

$$Q_s^{\mathfrak{m}}(\mathbf{X}\varphi) \approx \sum_{s' \in \mathrm{Sat}(\varphi)} \mathbf{Q}(s, s').$$

- **Until** bounded operator (***U*$^{\leq k}$**)*:* due to the finite nature of *k*, it's possible to accumulate the super-operators

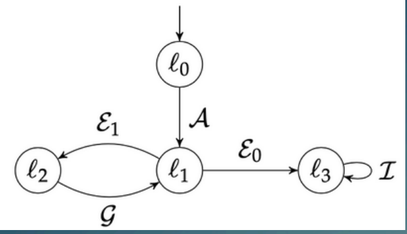
$$Q_s^{\mathfrak{m}}(\varphi_1 \mathbf{U}^{\leq k} \varphi_2) \eqsim \begin{cases} \mathcal{I}_{\mathcal{H}} & \text{if } s \in \mathrm{Sat}(\varphi_2); \\ \sum_{s' \in S} Q_{s'}^{\mathfrak{m}}(\varphi_1 \mathbf{U}^{\leq k-1} \varphi_2) \mathbf{Q}(s, s') & \text{if } k > 0 \text{ and } s \in \mathrm{Sat}(\varphi_1) \setminus \mathrm{Sat}(\varphi_2); \\ 0_{\mathcal{H}} & \text{otherwise.} \end{cases}$$

QCTL

- The last case is **Until** operator unbounded (**U**). The computation relies on fixed point. We start creating 3 sets:
  - $\mathcal{S}^{\mathcal{I}_\mathcal{H}}$, containing all states that surely satisfies the formula
  - $\mathcal{S}^{0_\mathcal{H}}$, containing all states that surely not satisfies the formula
  - $\mathcal{S}^{?}$, containing the remaining states.
- The superoperator used to assign this states is the least fixed point of function: $f(X) = X\mathcal{T} + \mathcal{G}$
  - The matrix $\mathcal{T}$ represents the super-operators that in one step leads to $\mathcal{S}^{?}$
  - The matrix $\mathcal{G}$ represents the super-operators that leads each state $s \in \mathcal{S}^{?}$ to goal set $\mathcal{S}^{\mathcal{I}_\mathcal{H}}$

QCTL example

```
ℓ0:  q := A(q);
ℓ1:  while M[q] do
ℓ2:      q := G(q);
ℓ3:  end
```



$$\mathbb{Q}_{\gtrsim \mathcal{I}_\mathcal{H}}[(\neg \ell_2)\mathbf{U}\ell_3]$$

$$\mathrm{Sat}(\ell_3) = \{\ell_3\} \quad \mathrm{Sat}(\neg \ell_2) = \{\ell_0, \ell_1, \ell_3\}$$

$$\mathcal{S}^{\mathcal{I}_\mathcal{H}} = \{\ell_3\} \quad \mathcal{S}^{0_\mathcal{H}} = \{\ell_2\} \quad \mathcal{S}^{?} = \{\ell_0, \ell_1\}$$

$$X_{\ell_0} \simeq \mathcal{E}_0\mathcal{A} \quad X_{\ell_1} \simeq \mathcal{E}_0 \implies X_{\ell_0} \not\gtrsim \mathcal{I}_\mathcal{H}, X_{\ell_1} \not\gtrsim \mathcal{I}_\mathcal{H},$$

$$\implies \mathrm{Sat}(\mathbb{Q}_{\gtrsim \mathcal{I}_\mathcal{H}}[(\neg \ell_2)\ \mathrm{U}\ \ell_3]) = \{\ell_3\}$$

FQCTL

QCTL is not able to characterize the effect of the super-operators on quantum states, unless this effect is reflected on the probability value. In other word, things like a bit flip remains **undetected**.
We need a different operators, called *Fidelity operator,* that give name to this logic.

- The only difference with QCTL is that the operator $\mathbb{Q}_{\sim\mathcal{E}}[\psi]$ is replaced with $\mathbb{F}_{\sim\tau}[\psi]$

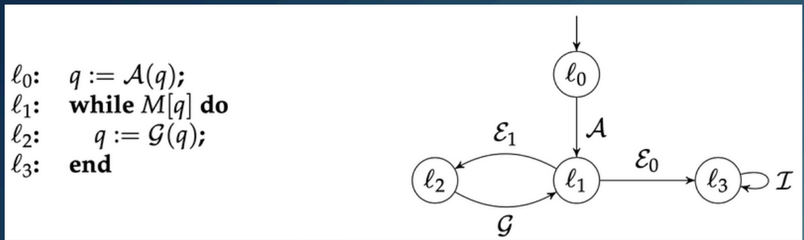
$$s \models \mathbb{F}_{\sim\tau}[\psi] \quad \text{if } \underline{\mathrm{Fid}}(Q_s^{\mathfrak{M}}(\{\sigma \in \mathrm{Path}^{\mathfrak{M}} \mid \sigma \models \psi\})) \sim \tau;$$

Given a super-operator, the Fid operator is defined as:

$$\underline{\mathrm{Fid}}(\mathcal{E}) = \min_{\rho \in \mathcal{D}^1(\mathcal{H})} \mathrm{Fid}(\mathcal{E}, \rho)$$

$$\text{where} \qquad \mathrm{Fid}(\mathcal{E}, \rho) = \sqrt{\rho^{1/2}\mathcal{E}(\rho)\rho^{1/2}}.$$

FQCTL example



$$\mathbb{F}_{\geq 1}[(\neg \ell_2)\mathbf{U}\ell_3]$$

$$\mathrm{Sat}(\ell_3) = \{\ell_3\} \quad \mathrm{Sat}(\neg \ell_2) = \{\ell_0, \ell_1, \ell_3\}$$

Let's now compute the super-operators corresponding to the path formula:

$$X_{\ell_0} \simeq \mathcal{E}_0 A \quad X_{\ell_1} \simeq \mathcal{E}_0 \quad X_{\ell_2} \simeq 0_{\mathcal{H}} \quad X_{\ell_3} \simeq \mathcal{I}_{\mathcal{H}}$$

The formula holds if the corresponding super opertor $X$is such that

$$\underline{Fid}(X_{\ell_i}) \geq 1$$

This holds only if $X_{\ell_i} \simeq \mathcal{I}_{\mathcal{H}}$ so only for ℓ_3

LTL

LTL and ω-regular properties are well suited for describing the behavior of a system in the long run.

$$\varphi ::= a \mid \varphi \wedge \varphi \mid \neg\varphi \mid \mathbf{X}\varphi \mid \varphi \,\mathbf{U}\, \varphi$$

- *a* is taken from a set of finite atomic propositions
- We call *word* an infinite sequence of atomic propositions

$$\begin{aligned}
w &\models a && \text{if } a \in w[0]; \\
w &\models \varphi_1 \wedge \varphi_2 && \text{if } w \models \varphi_1 \text{ and } w \models \varphi_2; \\
w &\models \neg\varphi && \text{if it is not the case that } w \models \varphi; \\
w &\models \mathbf{X}\varphi && \text{if } w[1..] \models \varphi; \text{ and} \\
w &\models \varphi_1 \,\mathbf{U}\, \varphi_2 && \text{if } \exists n \in \mathbb{N} : w[n..] \models \varphi_2 \text{ and } \forall 0 \leq i < n : w[i..] \models \varphi_1
\end{aligned}$$

LTL

Let $\mathfrak{M}$ be an LQMC, $s \in \mathcal{S}$ be a state, and φ be an LTL formula. Given $\sim \in \{\leq, \geq, \approx\}$ and $\mathcal{E} \in \mathcal{S}^{\mathcal{I}}(\mathcal{H})$, the model checking problem for $\mathfrak{M}$ against φ asks to verify whether $Q_s^{\mathfrak{M}}(\{\sigma \in \mathrm{Path}^{\mathfrak{M}} \mid L(\sigma) \in \mathrm{Words}(\varphi)\}) \sim \mathcal{E}$ holds.

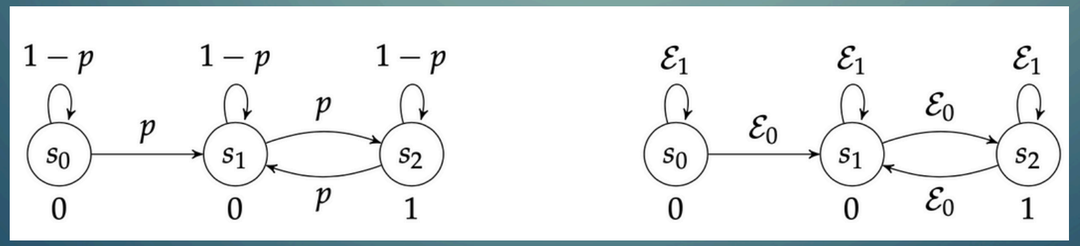
Let $\mathfrak{M}$ be an LQMC, $s \in \mathcal{S}$ be a state, and $\mathcal{W} \subseteq (2^{\mathrm{AP}})^{\omega}$ be an ω-regular property. Given $\sim \in \{\leq, \geq, \approx\}$ and $\mathcal{E} \in \mathcal{S}^{\mathcal{I}}(\mathcal{H})$, the model checking problem for $\mathfrak{M}$ against $\mathcal{W}$ asks to verify whether $Q_s^{\mathfrak{M}}(\{\sigma \in \mathrm{Path}^{\mathfrak{M}} \mid L(\sigma) \in \mathcal{W}\}) \sim \mathcal{E}$ holds.

LTL

- The standard approach requires to transform the LTL formula into an equivalent nondeterministic Büchi automaton accepting the same language as the original formula.
- This nondeterministic automaton is transformed into an equivalent deterministic automaton.
- The **parity Markov chain** is constituted by the Markov chain extended with the information about the accepted paths in automaton.
  - The paths are infinite, so to calculate the probability of an accepting path we use the **BSCC** (*bottom strongly connected component*).
  - Each BSCC is marked as accepting or rejecting

LTL

Consider this example. This will show why this approach cannot be used in QMC.



A path is accepted if the minimum proprity occurring infinitely often is even

- $s_0s_1s_2s_1s_2$ is accepted, s_2s_2 no
- s_0 in classical is a transient state (will reach surely the BSCC), so its priority is useless

The problems using this approach in QMC are:

- a state in QMC **cannot be classified** either as transient or as belonging to a BSCC
- the infinite path $(s_0)^\omega$ has minimum priority 0 so must be taking into account computing the superoperator corresponding to the accepting paths
- The graph is dynamic

Parity Automata

A (deterministic) *parity automaton* (PA) is a tuple $\mathfrak{A} = (A, \bar{a}, AP, t, \mathrm{pri})$, where:

- A is a *finite set* of automaton states;
- $\bar{a} \in A$ is the *initial state*;
- AP is a *finite set of atomic propositions*;
- $t : A \times 2^{AP} \to A$ is a *transition function*
- $\mathrm{pri} : A \to \mathbb{N}$ is a *priority function.*

- A path is an infinite sequence: $\sigma = a_0 L_0 a_1 L_1 \cdots \in (A \times 2^{AP})^\omega, | a_0 = \bar{a} \wedge \forall i \geq 0, a_{i+1} = t(a_i, L_i)$
- The priority function can be extended to paths: $\mathrm{pri}(\sigma) = \liminf_{i \to \infty} \mathrm{pri}(a_i)$
- The language of a parity atomaton is:

$$\mathcal{L}(\mathfrak{A}) = \{L_0 L_1 \cdots \in (2^{AP})^\omega \mid \exists \sigma = a_0 L_0 a_1 L_1 \cdots \in \mathrm{Path}^{\mathfrak{A}} : \mathrm{pri}(\sigma) \text{ is even}\}.$$

Parity QMC

A parity quantum Markov chain (PQMC) is a tuple $\mathfrak{M} = (S, Q, \mathrm{pri})$,
where (S, Q) is a QMC and $\mathrm{pri} : S \to \mathbb{N}$ is a priority function.

The value of PQMC in s ∈ S is: $\mathrm{val}_s^{\mathfrak{M}} = Q_s^{\mathfrak{M}}(\{\sigma \in \mathrm{Path}^{\mathfrak{M}} \mid \mathrm{pri}(\sigma) \text{ is even}\})$.
The PQMC can be obtained comining togheter LQMC and PA:

The product of an LQMC $\mathfrak{M} = (S, Q, AP, L)$ and a PA $\mathfrak{A} = (A, \bar{a}, AP, t, \mathrm{pri})$
with the same set of atomic propositions AP is the PQMC $\mathfrak{M} \otimes \mathfrak{A} = (S', Q', \mathrm{pri}')$ where

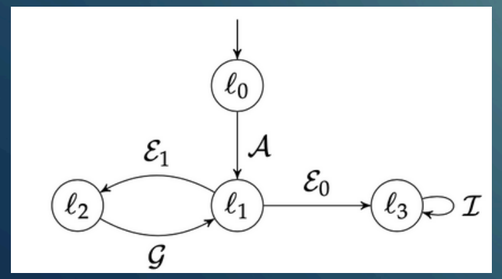
- $S' = S \times A$;
- $Q'((s,a),(s',a')) = Q(s,s')$ if $a' = t(a, L(s))$, and $Q'((s,a),(s',a')) = 0_{\mathcal{H}}$ otherwise;
- $\mathrm{pri}'((s,a)) = \mathrm{pri}(a)$.

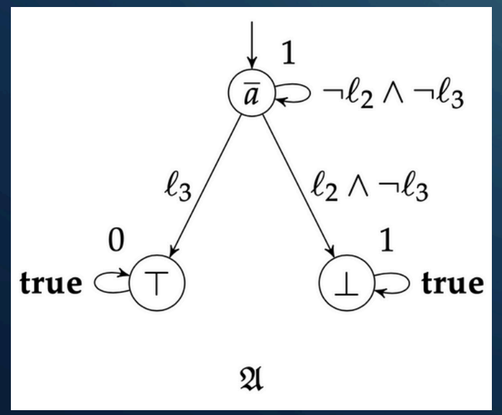
An important property that is used in the model checking problem of an LQMC against an ω-regular property $\mathscr{W}$ is that the value is **trace-equivalent** to the super-operator corresponding to $\mathscr{W}$ in LQMC.
This ensured the correctness of automata-based approach to model checking.

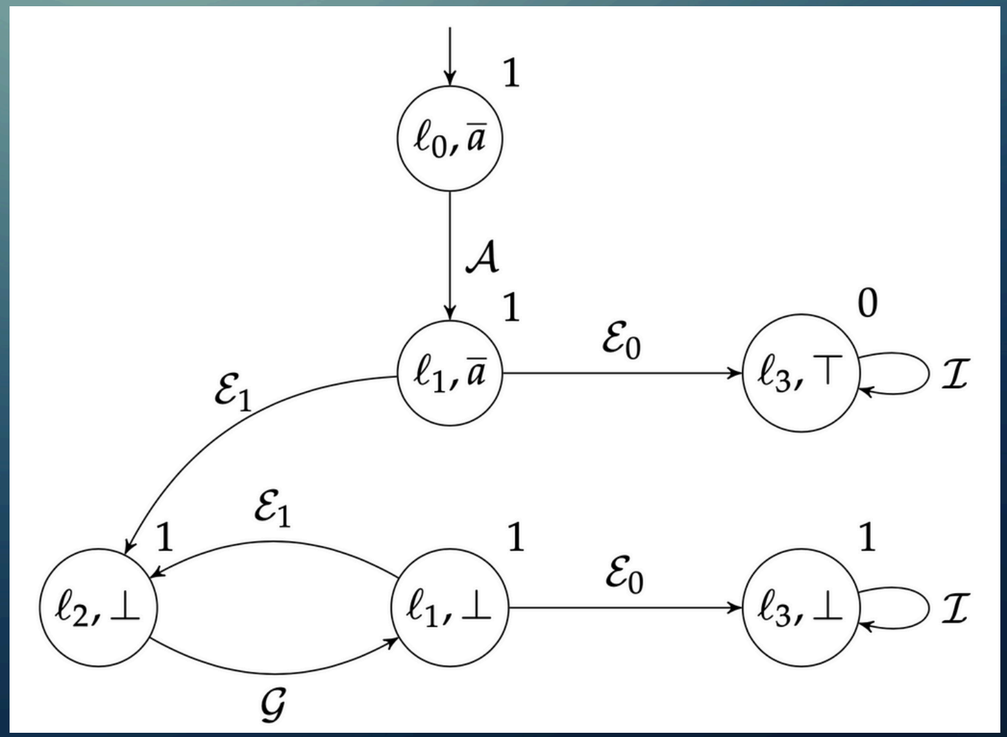
$$Q_s^{\mathfrak{M}}(\mathcal{L}(\mathfrak{A})) \sim \mathrm{val}_{(s,\bar{a})}^{\mathfrak{M}\otimes\mathfrak{A}}.$$

PQMC - example

Consider this QMC and the formula $(\neg \ell_2)\mathbf{U}\ell_3$







PQMC

Since it is not enough to compute BSCCs by looking only at the classical states, the intuition is to **extend** the Hilbert Space in order to keep track of classical state reached step by step:

$$\mathcal{H}_c \otimes \mathcal{H}$$

We need to unify the behaviour of the PQMC into a **unique** super-operator:

$$\mathcal{E}_{\mathfrak{M}} = \{|t\rangle\langle s| \otimes \mathcal{E}^{s,t}\}$$

- $\mathcal{E}^{s,t}$ is the super-operator linked to transitions from classical state *s* to classical state *t* (**Q***(s,t)*)
- $|t\rangle\langle s|$ "check" if the actual state is *s* and, if so, "transform" to state *t*

So this super-operator calculates a single step of system's evolution

PQMC

Now it's possible to search and classify a BSCC. In this context, a BSCC is a **subspace** instead of set of states.

- **invariant** subspace: when the system's evolution reach this subspace, it can't get out.$\mathcal{E}(X) \subseteq X$
- It is calculated based on a fixed point operator.

Given a BSCC B, the set *C(B)* contains all classical states supported in B.
Given all BSCCs of $\mathcal{E}_{\mathfrak{M}}$, these can be classified respect to the minimal priority assigned in each BSCC:

$$\mathcal{BSCC}_{=k} = \bigvee \{B \mid B \text{ is a BSCC of } \mathcal{E}_{\mathfrak{M}} \mid \min\{\mathrm{pri}(s) \mid s \in C(B)\} = k\}$$

This classification allows us to decompose the space:

$$\mathcal{H}_c \otimes \mathcal{H} = T \oplus \mathcal{BSCC}_{=k} \oplus \mathcal{BSCC}_{<k} \oplus \mathcal{BSCC}_{>k}$$

- The system will exit from the subspace T
- If the system reaches $BSCC_{<k}$ or $BSCC_{>k}$ the probability that we see *k* as minimum priority is 0
- If the system reaches $BSCC_{=k}$ then the probability that we see *k* as minimum priority is 1

PQMC

Let $\mathfrak{M} = (S, Q, \mathrm{pri})$ be a PQMC. Then, for any $s \in S$,

$$val_s^{\mathfrak{M}} \approx tr_c \circ \mathcal{P}_{even} \circ \mathcal{E}_{\mathfrak{M}}^{\infty} \circ \mathcal{E}_s$$

- tr_c is the partial trace operator. This operators discards the classica part to extrapolate the quantum one;
- $\mathcal{P}_{even} = \sum_{\{k \in \mathrm{pri}(S) | k \text{ is even}\}} \mathcal{P}_{=k}$ is the projective part that filters system's evolutions based on accepting conditions.
- $\mathcal{E}_{\mathfrak{M}}^{\infty} = \lim_{N \to \infty} \frac{1}{N} \sum_{n=1}^{N} \mathcal{E}_{\mathfrak{M}}^{n}$ simulates the system's evolution, showing how this is distributed among all BSCCs
- $\mathcal{E}_s$ creates the initial state of extended space starting from the quantum and the classical one

THANKS FOR ATTENTION