1 Quantum Markov Chains

Definition 1 *A quantum Markov chain* (QMC *for short*) $\mathcal{M}$ *is a triple* $(S, \boldsymbol{Q}, L)$*, in which*

- S *is a finite set of states,*
- $\boldsymbol{Q} : S \times S \to \mathcal{SO}(\mathcal{H})$ *is a transition super-operator matrix where for each* $s \in S$*,* $\sum_{t \in S} \boldsymbol{Q}[s,t] \approx \mathcal{I}$*, and*
- $L : S \to 2^{AP}$ *is a labelling function.*

The transition super-operator matrix **Q** in a QMC is functionally analogous to the transition probability matrix in a classical Markov chain (MC).

Example 1 (Quantum loop programs, already in ePMC) A simple quantum loop program reads as follows:

$$\begin{aligned}
&l_0 : q := \mathcal{F}(q);\\
&l_1 : \textbf{while } M[q] \textbf{ do}\\
&l_2 : \qquad q := \mathcal{E}(q);\\
&l_3 : \textbf{end}
\end{aligned}$$

where $M = 0 \cdot |0\rangle\langle 0| + 1 \cdot |1\rangle\langle 1|$.

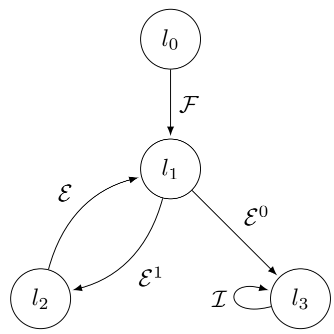

Fig. 1. The QMC for a quantum loop program.

Example 2 (Quantum recursive programs) Suppose Alice and Bob want to randomly choose a leader between them, by taking a qubit system q as the coin. The protocol of Alice goes as follows. She first measures the system q according to the observable $M_A = 0 \cdot |\psi\rangle\langle\psi| + 1 \cdot |\psi^\perp\rangle\langle\psi^\perp|$ where $\{|\psi\rangle, |\psi^\perp\rangle\}$ is an orthonormal basis of $\mathcal{H}_q$. If the outcome 0 is observed, then she is the winner. Otherwise, she gives the quantum system q to Bob and lets him decide. Bob's protocol goes similarly, except that his measurement operator is $M_B = 0 \cdot |\varphi\rangle\langle\varphi| + 1 \cdot |\varphi^\perp\rangle\langle\varphi^\perp|$ for another orthonormal basis $\{|\varphi\rangle, |\varphi^\perp\rangle\}$ of $\mathcal{H}_q$ so that $|\langle\psi|\varphi\rangle| \notin \{0, 1\}$.

We can describe such a protocol as the following quantum program with procedure calls.

Global variables $winner$: string, q : **qubit**	
Program Alice	**Program** Bob
switch $M_A[q]$ **do**	**switch** $M_B[q]$ **do**
case 0	**case** 0
$winner :=$ 'A';	$winner :=$ 'B';
case 1	**case** 1
Call Bob;	Call Alice;
end	**end**

The semantics of this program can be described by a QMC depicted in Fig. 2 where the transition super-operator matrix **Q** is given by:

$$\mathbf{Q}[s_a, t_a] = \{|\psi\rangle\langle\psi|\}, \quad \mathbf{Q}[s_a, s_b] = \{|\psi^\perp\rangle\langle\psi^\perp|\},$$
$$\mathbf{Q}[s_b, t_b] = \{|\varphi\rangle\langle\varphi|\}, \quad \mathbf{Q}[s_b, s_a] = \{|\varphi^\perp\rangle\langle\varphi^\perp|\}.$$

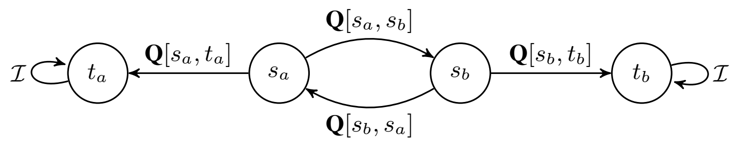

Fig. 2. The QMC for a leader election protocol.

Intuitively, the state s_a (resp. s_b) corresponds to the position in the program where Alice (reps. Bob) is about to perform the measurement M_A (resp. M_B), while the state t_a (resp. t_b) corresponds to Alice (reps. Bob) being selected to be the winner.

Example 3 (Quantum key-distribution protocol) Already in ePMC; omit the description here.

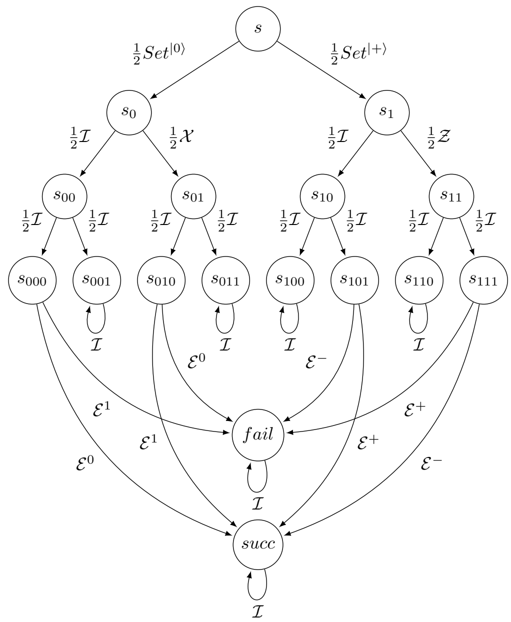

Fig. 3. The QMC for the basic BB84 protocol when $n = 1$.

2 Linear Temporal Logic

The syntax of Linear Temporal Logic (LTL) is given in the following:

$$\psi ::= a \mid \neg\psi \mid \psi_1 \wedge \psi_2 \mid \mathbf{X}\psi \mid \psi_1 \mathbf{U} \psi_2$$

where $a \in AP$. We introduce some syntactic sugars to simplify notations: the falsility $\texttt{ff} \equiv a \wedge \neg a$, the tautology $\texttt{tt} \equiv \neg\texttt{ff}$, the disjunction $\psi_1 \vee \psi_2 \equiv \neg(\neg\psi_1 \wedge \neg\psi_2)$, the *eventually* operator $\Diamond\psi \equiv \texttt{tt}\mathbf{U}\psi$, and the *always* operator $\Box\psi \equiv \neg\Diamond\neg\psi$.

The LTL model checking problem is that given a QMC $\mathcal{M} = (S, \mathbf{Q}, L)$, $s \in S$, and an LTL formula ψ, compute a matrix corresponding to all paths of $\mathcal{M}$ satisfying ψ:

$$\mathrm{Qr}_s^{\mathcal{M}}(\psi) := \Delta_s^{\mathcal{M}}(\{\pi \in \mathrm{Path}^{\mathcal{M}}(s) \mid \pi \models \psi\}).$$

Example 4 *1. The LTL formula $\Diamond l_3$ denotes the property that the loop program in Example 1 terminates.*

2. The LTL formulas $\Diamond t_a$ denotes the event that Alice is eventually selected as the winner; similarly for $\Diamond t_b$.

3. The LTL formulas $\Diamond fail$ and $\Diamond succ$ denotes the events that the basic BB84 protocol fails and succeeds, respectively.

3 Algorithms for Model Checking

Algorithm 1: Algorithms for model checking LTL formulas

input : A QMC $\mathcal{M}$ and an LTL formula ψ.
output: A matrix.
begin
  Construct a parity automaton $\mathcal{A}$ from ψ (This part is purely classical);
  Construct the product automaton $\mathcal{M} \otimes \mathcal{A}$ (Definition 4 below);
  Use Algorithm 2 to compute the value M of $\mathcal{M} \otimes \mathcal{A}$ at $(s, \overline{a})$;
  return M
end

Definition 2 (Parity Automaton) *A* (deterministic) parity automaton *(PA) is a tuple $\mathcal{A} = (A, \overline{a}, t, \mathsf{pri})$, where*

1. *A is a finite set of automaton states, and $\overline{a} \in A$ is the* initial state*,*
2. *$t\colon A \times 2^{AP} \to A$ is a* transition function*,*
3. *$\mathsf{pri}\colon A \to \mathbb{N}$ is a* priority function*. Here $\mathbb{N}$ denotes the set of natural numbers.*

A path *of $\mathcal{A}$ is an infinite sequence $\pi = a_0 L_0 a_1 L_1 \ldots \in (A \times 2^{AP})^\omega$ such that $a_0 = \overline{a}$ and for all $i \geq 0$, $t(a_i, L_i) = a_{i+1}$. We extend the priority function to paths by setting $\mathsf{pri}(\pi) = \liminf_{i\to\infty} \mathsf{pri}(a_i)$. We use $\mathrm{Path}^{\mathcal{A}}$ to denote the set of all paths of $\mathcal{A}$. The* language *of $\mathcal{A}$ is defined as*

$$\mathcal{L}(\mathcal{A}) = \{\, L_0 L_1 \ldots \in (2^{AP})^\omega \mid \exists \pi = a_0 L_0 a_1 L_1 \ldots \in \mathrm{Path}^{\mathcal{A}}.\ \mathsf{pri}(\pi) \text{ is even} \,\}.$$

Definition 3 (Parity QMC) *A parity QMC (*PQMC*) is a tuple $\mathcal{M} = (S, \boldsymbol{Q}, L, \mathsf{pri})$, where $(S, \boldsymbol{Q}, L)$ is a* QMC *and $\mathsf{pri}\colon S \to \mathbb{N}$ is a* priority function *for the classical states. We define the* value *of $\mathcal{M}$ in $s \in S$ as*

$$\mathrm{val}_s^{\mathcal{M}} = \Delta_s^{\mathcal{M}}(\{\, \pi \in \mathrm{Path}^{\mathcal{M}} \mid \mathsf{pri}(\pi) \text{ is even} \,\}).$$

Here again, we set $\mathsf{pri}(\pi) = \liminf_{i\to\infty} \mathsf{pri}(s_i)$ provided that $\pi = s_0 s_1 s_2 \ldots$.

Definition 4 (QMC-PA Product) *The* product *of an* QMC *$\mathcal{M} = (S, \boldsymbol{Q}, L)$ and a PA $\mathcal{A} = (A, \overline{a}, t, \mathsf{pri})$ with the same set AP of atomic propositions is a* PQMC *$\mathcal{M} \otimes \mathcal{A} = (S', \boldsymbol{Q}', \mathsf{pri}')$ where*

1. *$S' = S \times A$,*
2. *$\boldsymbol{Q}'((s, a), (s', a')) = \boldsymbol{Q}(s, s')$ if $t(a, L(s)) = a'$, and 0 otherwise,*
3. *$\mathsf{pri}'((s, a)) = \mathsf{pri}(a)$.*

Theorem 1 *Consider the product $\mathcal{M}' = \mathcal{M} \otimes \mathcal{A} = (S', \boldsymbol{Q}', \mathsf{pri}')$ of a* QMC *$\mathcal{M} = (S, \boldsymbol{Q}, L)$ and a PA $\mathcal{A} = (A, \overline{a}, t, \mathsf{pri})$ which is produced from LTL formula ψ. Then for any $s \in S$,*

$$\mathrm{Qr}_s^{\mathcal{M}}(\psi) = \mathrm{val}_{(s,\overline{a})}^{\mathcal{M}'}.$$

Algorithm 2: Compute the values of a PQMC

```
input  : A PQMC M = (S, Q, pri) on H and a classical state s ∈ S.
output: Value of M at s.
begin
    (* Compute E_M and E_M^∞ *)
    E_M ← 0;
    for t, t' ∈ S do
        E_M ← E_M + {|t'⟩⟨t|} ⊗ Q[t, t'];
    end
    E_M^∞ ← the super-operator determined by its matrix representation given in Eq.(??);

    (* Compute P_even *)
    P_even ← 0; I_c ← Σ_{t∈S} |t⟩⟨t|;
    B ← GetBSCCs(E_M, I_c ⊗ I_H);
    EP ← { pri(t) | t ∈ S ∧ pri(t) is even };
    for k ∈ EP do
        P_k ← 0;
        for B ∈ B with k = min{ pri(t) | t ∈ C(B) } do
            P_k ← P_k + P_B where P_B is the projector onto B;
        end
        P_even ← P_even + P_k;
    end

    M ← E_M^∞†(P_even);
    return ⟨s| ⊗ I_H · M · |s⟩ ⊗ I_H
end
```

Let $\mathcal{M} = (S, \mathbf{Q}, \mathsf{pri})$ be a PQMC on $\mathcal{H}$ with $\mathbf{Q}(s,t) = \{ E_i^{s,t} \mid i \in I^{s,t} \}$. We define a super-operator

$$\mathcal{E}_{\mathcal{M}} = \{ |t\rangle\langle s| \otimes E_i^{s,t} \mid s, t \in S, i \in I^{s,t} \} \tag{1}$$

acting on the Hilbert space $\mathcal{H}_c \otimes \mathcal{H}$, where $\mathcal{H}_c$ is a $|S|$-dimensional Hilbert space with an orthonormal basis $\{ |s\rangle \mid s \in S \}$. For a BSCC B of $\mathcal{E}_{\mathcal{M}}$, let

$$C(B) = \{ s \in S \mid |s\rangle|\psi\rangle \in B \text{ for some } |\psi\rangle \in \mathcal{H} \}$$

be the set of classical states supported in B.

Theorem 2 *Let $\mathcal{M} = (S, \boldsymbol{Q}, \mathsf{pri})$ be a* PQMC. *Then for any $s \in S$,*

$$\mathrm{val}_s^{\mathcal{M}} = \mathcal{E}_s^\dagger \circ {\mathcal{E}_{\mathcal{M}}^{\infty}}^\dagger(P_{even})$$

where $\mathcal{E}_{\mathcal{M}}^{\infty} = \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \mathcal{E}_{\mathcal{M}}^n$, $P_{even} = \sum_{\{ k \in \mathsf{pri}(S) | k \text{ is even} \}} P_k$, and $\mathcal{E}_s(\rho) = |s\rangle\langle s| \otimes \rho$ for all $\rho \in \mathcal{D}(\mathcal{H})$.

Example 5 *Let $\mathcal{M}_i$ be the QMCs given in the three examples above (the models in Examples 1 and 3 have already used in ePMC [QCTL model checker part]). Then*

1. *for any $s \in \{l_i : i = 0 \cdots 3\}$, $\mathrm{Qr}_s^{\mathcal{M}_1}(\Diamond l_3) = I$.*
2. $\mathrm{Qr}_{s_a}^{\mathcal{M}_2}(\Diamond t_a) = |0\rangle\langle 0| + \frac{1}{3}|1\rangle\langle 1|$, $\mathrm{Qr}_{s_b}^{\mathcal{M}_2}(\Diamond t_a) = \frac{2}{3}|-\rangle\langle -|$, $\mathrm{Qr}_{s_a}^{\mathcal{M}_2}(\Diamond t_b) = \frac{2}{3}|1\rangle\langle 1|$, *and* $\mathrm{Qr}_{s_b}^{\mathcal{M}_2}(\Diamond t_b) = |+\rangle\langle +| + \frac{1}{3}|-\rangle\langle -|$.
3. $\mathrm{Qr}_s^{\mathcal{M}_3}(\Diamond fail) = 0$ *and* $\mathrm{Qr}_s^{\mathcal{M}_3}(\Diamond succ) = I/2$.

Example 6 *Let $\mathcal{M}$ be depicted in Fig.4, and $\psi = \Box(s_0 \wedge \neg s_1)$. Then $\mathrm{Qr}_{s_0}^{\mathcal{M}}(\psi) = |0\rangle\langle 0|$ and $\mathrm{Qr}_{s_1}^{\mathcal{M}}(\psi) = 0$.*

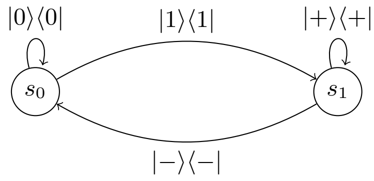

Fig. 4. QMC for Example 6.

Procedure GetBSCCs($\mathcal{E}, P$)

---

input : A super-operator $\mathcal{E}$ acting on $\hat{\mathcal{H}}$, and a projector P to some invariant subspace $\mathcal{H}' \subseteq \hat{\mathcal{H}}$ of $\mathcal{E}$.
output: A complete set of orthogonal BSCCs of $\mathcal{E}$ in $\mathcal{H}'$.
begin
  $\mathcal{X} \leftarrow$ a basis of $\{ X \in \mathcal{L}(\mathcal{H}') \mid \mathcal{E}(X) = X \}$;
  $F \leftarrow \emptyset$;
  for $X \in \mathcal{X}$ **do**
    $X_R \leftarrow (X + X^\dagger)/2$; $X_I \leftarrow (X - X^\dagger)/2i$;
      (* $X^\dagger$ denotes the transpose and complex conjugate of X *)
    $P_R^+ \leftarrow$ the projector onto eigenspace of X_R with positive eigenvalues;
    $P_I^+ \leftarrow$ the projector onto eigenspace of X_I with positive eigenvalues;
    $X_R^+ = P_R^+ X_R P_R^+$; $X_R^- = X_R^+ - X_R$;
    $X_I^+ = P_I^+ X_I P_I^+$; $X_I^- = X_I^+ - X_I$;
      (* All of them are positive semidefinite, and $X = X_R^+ - X_R^- + i(X_I^+ - X_I^-)$ *)
    for $Y \in \{X_R^+, X_R^-, X_I^+, X_I^-\} \wedge Y \neq 0$ **do**
      $F \leftarrow F \cup \{Y/\mathrm{tr}(Y)\}$; (* Fixed point states of $\mathcal{E}$ *)
    end
  end
  if $|F| = 1$ **then**
    return $\{\mathrm{supp}(Y)\}$; (* Y is the only element of F *)
  else
    $Y_1, Y_2 \leftarrow$ two arbitrary different elements of F;
    $P^+ \leftarrow$ the projector onto eigenspace of $Y_1 - Y_2$ with positive eigenvalues;
    $P^- \leftarrow P - P^+$;
    $\mathcal{E}^+ \leftarrow \mathcal{P}^+ \circ \mathcal{E}$; (* $\mathcal{P}^+$ is the super-operator $\{P^+\}$ *)
    $\mathcal{E}^- \leftarrow \mathcal{P}^- \circ \mathcal{E}$; (* $\mathcal{P}^-$ is the super-operator $\{P^-\}$ *)
    return GetBSCCs($\mathcal{E}^+, P^+$) $\cup$ GetBSCCs($\mathcal{E}^-, P^-$);
  end
end
