Symbolic Model Checking Quantum Circuits With Density Operators in Maude

Canh Minh Do   Kazuhiro Ogata

Japan Advanced Institute of Science and Technology, 1-8 Asahidai, Nomi, Japan

Presented Physically at the 2nd International Workshop on Formal Analysis and Verification of Post-Quantum Cryptographic Protocols

November 21, 2023 - Brisbane, Australia

Contents

Contents

Introduction

- Quantum computing is a rapidly emerging technology that uses the laws of quantum mechanics to solve complex problems beyond the capabilities of classical computers, such as Shore's fast algorithms[1] for discrete logarithms and factoring.
- Quantum circuits are a model of quantum computation used to design and implement quantum algorithms, programs, and protocols.
- Due to radically different principles of quantum mechanics, such as superposition, entanglement, and measurement, it is challenging to accurately design and implement quantum algorithms, quantum programs, and quantum protocols.
- Therefore, it is crucial to ensure the correctness of quantum circuits through verification.

[1] P.W. Shor. "Algorithms for quantum computation: discrete logarithms and factoring". In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. 1994.

Model Checking Quantum Circuits

- We proposed a symbolic approach to model checking quantum circuits with a support tool implemented in Maude with pure states[2], but not mixed states.
- In many practical situations, a quantum system is not a single, well-defined state but a statistical mixture of multiple pure states (also called mixed states).
- This motivated us to extend our symbolic model checking quantum circuits to handle mixed states by using density operators.

[2] Canh Minh Do and Kazuhiro Ogata. "Symbolic Model Checking Quantum Circuits in Maude". In: *The 35th International Conference on Software Engineering and Knowledge Engineering, SEKE 2023*. 2023.

Contents

Hilbert Spaces

- A Hilbert space $\mathcal{H}$ usually serves as the state space of a quantum system that is a complex vector space equipped with an inner product such that each Cauchy sequence of vectors has a limit.
- An n-qubit system is the complex 2^n-space $\mathbb{C}^{2^n}$, where $\mathbb{C}$ stands for the complex plane.
- Pure states in the n-qubit systems $\mathbb{C}^{2^n}$ are unit vectors in 2^n-space $\mathbb{C}^{2^n}$.
- The orthogonal basis called computational basis in the one-qubit system $\mathbb{C}^2$ is the set $\{|0\rangle, |1\rangle\}$ that consists of the column vectors $|0\rangle = (1, 0)^T$ and $|1\rangle = (0, 1)^T$, where ^{T} denotes the transpose operator.
- In the two-qubit system $\mathbb{C}^4$, there are pure states that cannot be represented in the form $|\psi_1\rangle \otimes |\psi_2\rangle$ and called entangled states, where $\otimes$ denotes the tensor product (more precisely, the Kronecker product).
- For example, the EPR state (Einstein-Podolsky-Rosen state) $|EPR\rangle = (|00\rangle + |11\rangle)/\sqrt(2)$ is an entangled state, where $|00\rangle = |0\rangle \otimes |0\rangle$ and $|11\rangle = |1\rangle \otimes |1\rangle$.

Unitary Operators

- Quantum computation is represented by unitary operators (also called quantum gates).
- For example, the Hadamard gate H and Pauli gates X, Y, and Z are quantum gates on the one-qubit system $\mathbb{C}^2$ and are defined as follows:

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

- Two typical quantum gates on the two-qubit systems $\mathbb{C}^4$ are the controlled-X gate (also called the controlled-NOT gate) CX and the swap gate $SWAP$ are defined by

$$\begin{aligned} CX &= |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X, \\ SWAP &= CX(I \otimes |0\rangle\langle 0| + X \otimes |1\rangle\langle 1|)CX, \end{aligned}$$

where I denotes the identity matrix of size 2×2.

Measurement

- Measurement is a completely different process from applying quantum gates. Here we roughly explain specific projective measurements.
- For the general definition of projective measurement, see the famous textbook of quantum computation[3].
- Observe that $P_0 = |0\rangle\langle 0|$ and $P_1 = |1\rangle\langle 1|$ are projectors, respectively.
- After executing the measurement $\{P_0, P_1\}$, a current state $|\psi\rangle = c_0\,|0\rangle + c_1\,|1\rangle$ is collapsed into either $\frac{P_0|\psi\rangle}{|c_0|}$ with probability $|c_0|^2$ or into $\frac{P_1|\psi\rangle}{|c_1|}$ with probability $|c_1|^2$.

$$\begin{tikzcd} & \frac{c_0|0\rangle}{|c_0|} \approx |0\rangle \\ |\psi\rangle \arrow[ur, "|c_0|^2"] \arrow[dr, "|c_1|^2"'] & \\ & \frac{c_1|1\rangle}{|c_1|} \approx |1\rangle \end{tikzcd}$$

[3] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2010.

Pure States vs Mixed States

	Pure States	Mixed States
System information	Complete (a pure state $\|\psi\rangle$)	Partial (an ensemble of pure states $\{(p_i, \|\psi_i\rangle)\}$)
State representation	$\|\psi\rangle$	$\rho = \sum_i p_i \|\psi_i\rangle\langle\psi_i\|$
Unitary evolution	$\|\psi'\rangle = \boldsymbol{U} \|\psi\rangle$	$\rho' = \boldsymbol{U}\rho\boldsymbol{U}^\dagger$
Measurement $\{\boldsymbol{M}_m\}$	$p(m) = \langle\psi\| \boldsymbol{M}_m^\dagger \boldsymbol{M}_m \|\psi\rangle$ $\frac{\boldsymbol{M}_m\|\psi\rangle}{\sqrt{p(m)}}$	$p(m) = tr(\boldsymbol{M}_m^\dagger \boldsymbol{M}_m \rho)$ $\rho' = \frac{\boldsymbol{M}_m \rho \boldsymbol{M}_m^\dagger}{p(m)}$

- The trace $tr(\boldsymbol{A})$ of operator $\boldsymbol{A}$ is defined to be $tr(\boldsymbol{A}) = \sum_i \langle\phi_i|\boldsymbol{A}|\phi_i\rangle$ for some given orthonormal basis $\{|\phi_i\rangle\}$.
- ρ is called a density operator or density matrix satisfying the trace condition $tr(\rho) = 1$.

- The deepest application of the density operator is as a descriptive tool for sub-systems of a composite quantum system[4].

Reduced Density Operators

Let A and B be two quantum systems whose state is described by a density operator ρ^{AB}. The **reduced density operator** for system A is defined by

$$\rho^{A} = tr_B(\rho^{AB})$$

where tr_B is the **partial trace** over system B that is defined by

$$tr_B(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|) = |a_1\rangle\langle a_2| \, tr(|b_1\rangle\langle b_2|) = |a_1\rangle\langle a_2| \, \langle b_2|b_1\rangle$$

where $|a_1\rangle$ and $|a_2\rangle$ are any two vectors in the state space of A, and $|b_1\rangle$ and $|b_2\rangle$ are any two vectors in the state space of B.

[4] Nielsen and Chuang, *Quantum Computation and Quantum Information*.

Contents

Terms

Terms are built from scalars and basic vectors with some constructors.

- *Scalars* are complex numbers with some operations supported, such as multiplication, fraction, addition, conjugation, absolute, power, and square root.
- *Basic vectors* are the computational basis written in Dirac notation as $|0\rangle$ and $|1\rangle$.
- *Constructors* for matrices consist of scalar multiplication of matrices $\cdot$, matrix product $\times$, matrix addition $+$, tensor product $\otimes$, and the conjugate transpose $\boldsymbol{A}^\dagger$ of a matrix $\boldsymbol{A}$.

Terms

- We conventionally formalize some basic matrices $\boldsymbol{B}_i$ for $i \in [0..3]$ as follows:

$$\boldsymbol{B}_0 = |0\rangle \times \langle 0|\,, \quad \boldsymbol{B}_1 = |0\rangle \times \langle 1|\,, \quad \boldsymbol{B}_2 = |1\rangle \times \langle 0|\,, \quad \boldsymbol{B}_3 = |1\rangle \times \langle 1|$$

- The $\boldsymbol{X}$, $\boldsymbol{Y}$, $\boldsymbol{Z}$, $\boldsymbol{H}$, and $\boldsymbol{CX}$ gates are then a linear combination of the matrices $\boldsymbol{B}_i$ as follows:

$$\boldsymbol{X} = \boldsymbol{B}_1 + \boldsymbol{B}_2, \quad \boldsymbol{Y} = (-i) \cdot \boldsymbol{B}_1 + i \cdot \boldsymbol{B}_2, \quad \boldsymbol{Z} = \boldsymbol{B}_1 + (-1) \cdot \boldsymbol{B}_3,$$

$$\boldsymbol{H} = \frac{1}{\sqrt{2}} \cdot \boldsymbol{B}_0 + \frac{1}{\sqrt{2}} \cdot \boldsymbol{B}_1 + \frac{1}{\sqrt{2}} \cdot \boldsymbol{B}_2 + (-\frac{1}{\sqrt{2}}) \cdot \boldsymbol{B}_3, \quad \boldsymbol{CX} = \boldsymbol{B}_0 \otimes \boldsymbol{I}_2 + \boldsymbol{B}_3 \otimes \boldsymbol{X}$$

Laws

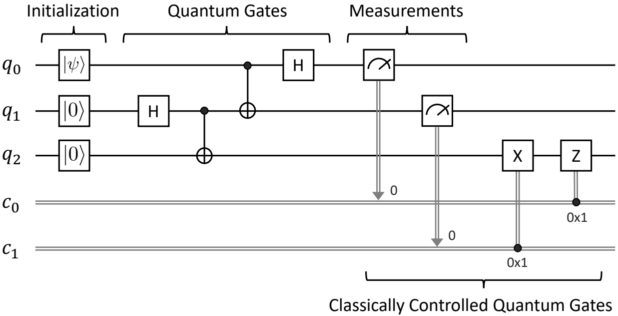
No.	Law
L1	$\langle 0\|0\rangle = \langle 1\|1\rangle = 1, \langle 1\|1\rangle = \langle 0\|1\rangle = 0$
L2	Associativity of $\times, +, \otimes$ and Commutativity of $+$
L3	$0 \cdot \boldsymbol{A}_{m\times n} = \mathrm{O}_{m\times n},\ c \cdot \mathrm{O} = \mathrm{O},\ 1 \cdot \boldsymbol{A} = \boldsymbol{A}$
L4	$c \cdot (\boldsymbol{A} + \boldsymbol{B}) = c \cdot \boldsymbol{A} + c \cdot \boldsymbol{B}$
L5	$c_1 \cdot \boldsymbol{A} + c_2 \cdot \boldsymbol{A} = (c_1 + c_2) \cdot \boldsymbol{A}$
L6	$c_1 \cdot (c_2 \cdot \boldsymbol{A}) = (c_1 \cdot c_2) \cdot \boldsymbol{A}$
L7	$(c_1 \cdot \boldsymbol{A}) \times (c_2 \cdot \boldsymbol{B}) = (c_1 \cdot c_2) \cdot (\boldsymbol{A} \times \boldsymbol{B})$
L8	$\boldsymbol{A} \times (c \cdot \boldsymbol{B}) = (c \cdot \boldsymbol{A}) \times \boldsymbol{B} = c \cdot (\boldsymbol{A} \times \boldsymbol{B})$
L9	$\boldsymbol{A} \otimes (c \cdot \boldsymbol{B}) = (c \cdot \boldsymbol{A}) \otimes \boldsymbol{B} = c \cdot (\boldsymbol{A} \otimes \boldsymbol{B})$
L10	$\mathrm{O}_{m\times n} \times \boldsymbol{A}_{n\times p} = \boldsymbol{A}_{m\times n} \times \mathrm{O}_{n\times p} = \mathrm{O}_{m\times p}$
L11	$\mathrm{I}_m \times \boldsymbol{A}_{m\times n} = \boldsymbol{A}_{m\times n} \times \mathrm{I}_n = \boldsymbol{A}_{m\times n}$
L12	$\boldsymbol{A} + \mathrm{O} = \mathrm{O} + \boldsymbol{A} = \mathrm{O}$
L13	$\mathrm{O}_{m\times n} \otimes \boldsymbol{A}_{p\times q} = \boldsymbol{A}_{p\times q} \otimes \mathrm{O}_{m\times n} = \mathrm{O}_{mp\times nq}$
L14	$\boldsymbol{A} \times (\boldsymbol{B} + \boldsymbol{C}) = \boldsymbol{A} \times \boldsymbol{B} + \boldsymbol{A} \times \boldsymbol{C}$
L15	$(\boldsymbol{A} + \boldsymbol{B}) \times \boldsymbol{C} = \boldsymbol{A} \times \boldsymbol{C} + \boldsymbol{B} \times \boldsymbol{C}$
L16	$(\boldsymbol{A} \otimes \boldsymbol{B}) \times (\boldsymbol{C} \otimes \boldsymbol{D}) = (\boldsymbol{A} \times \boldsymbol{C}) \otimes (\boldsymbol{B} \times \boldsymbol{D})$
L17	$\boldsymbol{A} \otimes (\boldsymbol{B} + \boldsymbol{C}) = \boldsymbol{A} \otimes \boldsymbol{B} + \boldsymbol{A} \otimes \boldsymbol{C}$
L18	$(\boldsymbol{A} + \boldsymbol{B}) \otimes \boldsymbol{C} = \boldsymbol{A} \otimes \boldsymbol{C} + \boldsymbol{B} \otimes \boldsymbol{C}$
L19	$(c \cdot \boldsymbol{A})^\dagger = c^* \cdot \boldsymbol{A}^\dagger,\ (\boldsymbol{A} \times \boldsymbol{B})^\dagger = \boldsymbol{B}^\dagger \times \boldsymbol{A}^\dagger$
L20	$(\boldsymbol{A} + \boldsymbol{B})^\dagger = \boldsymbol{A}^\dagger + \boldsymbol{B}^\dagger,\ (\boldsymbol{A} \otimes \boldsymbol{B})^\dagger = \boldsymbol{A}^\dagger \otimes \boldsymbol{B}^\dagger$
L21	$\boldsymbol{I}_m{}^\dagger = \boldsymbol{I}_m, \boldsymbol{O}_{m\times n}^\dagger = \boldsymbol{O}_{n\times m}, (\boldsymbol{A}^\dagger)^\dagger = \boldsymbol{A}$
L22	$\|0\rangle^\dagger = \langle 0\|,\ \langle 0\|^\dagger = \|0\rangle,\ \|1\rangle^\dagger = \langle 1\|,\ \langle 1\|^\dagger = \|1\rangle$

$$
\begin{aligned}
&\boldsymbol{H} \times |0\rangle \\
&= (\tfrac{1}{\sqrt{2}} \cdot \boldsymbol{B}_0 + \tfrac{1}{\sqrt{2}} \cdot \boldsymbol{B}_1 + \tfrac{1}{\sqrt{2}} \cdot \boldsymbol{B}_2 + (-\tfrac{1}{\sqrt{2}}) \cdot \boldsymbol{B}_3) \times |0\rangle \\
&= \tfrac{1}{\sqrt{2}} \cdot \boldsymbol{B}_0 \times |0\rangle + \tfrac{1}{\sqrt{2}} \cdot \boldsymbol{B}_1 \times |0\rangle + \tfrac{1}{\sqrt{2}} \cdot \boldsymbol{B}_2 \times |0\rangle \\
&+ (-\tfrac{1}{\sqrt{2}}) \cdot \boldsymbol{B}_3 \times |0\rangle \\
&= \tfrac{1}{\sqrt{2}} \cdot |0\rangle \times \langle 0| \times |0\rangle + \tfrac{1}{\sqrt{2}} \cdot |0\rangle \times \langle 1| \times |0\rangle \\
&+ \tfrac{1}{\sqrt{2}} \cdot |1\rangle \times \langle 0| \times |0\rangle + (-\tfrac{1}{\sqrt{2}}) \cdot |1\rangle \times \langle 1| \times |0\rangle \\
&= \tfrac{1}{\sqrt{2}} \cdot |0\rangle + \tfrac{1}{\sqrt{2}} \cdot |1\rangle
\end{aligned}
$$

Contents

Quantum Teleportation

- Alice wants to send an arbitrary pure state $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ to Bob.
- The no-cloning theorem states that we cannot make an extract copy of an unknown quantum state.
- Taking advantage of two classical bits and an entangled qubit pair, Alice can send the qubit $|\psi\rangle$ to Bob.



Formalization of Quantum Circuits

- *A whole quantum state* is formalized as a density operator representing a mixed state.
- *Classical bits* are formalized as a map from indices in circuits to Boolean values, where each entry is in the form of $(i \mapsto b)$, meaning that the value of the classical bit stored at c_i is b whose value is either 0 or 1.

Formalization of Quantum Circuits

A sequence of quantum gates, measurements, and *conditional gates* is formalized as a list of actions in which each action is one of the forms as follows:

- `X(`i`)` applies the X gate on qubit at index i,
- `Y(`i`)` applies the Y gate on qubit at index i,
- `Z(`i`)` applies the Z gate on qubit at index i,
- `H(`i`)` applies the H gate on qubit at index i,
- `CX(`i, j`)` applies the CX gate on qubits at indices i and j,
- `CY(`i, j`)` applies the CY gate on qubits at indices i and j,
- `CZ(`i, j`)` applies the CZ gate on qubits at indices i and j,
- `SWAP(`i, j`)` applies the SWAP gate on qubits at indices i and j,
- `CCX(`i, j, k`)` applies the CCX gate on qubits at indices i, j and k,
- `CCZ(`i, j, k`)` applies the CCX gate on qubits at indices i, j and k,
- `CSWAP(`i, j, k`)` applies the CSWAP gate on qubits at indices i, j and k,
- `M(`i`)` measures q_i with the computational basis,
- `c[`i`] ==`b`? AL` checks if c_i equals b, then a list `AL` of actions is executed.

A Kripke Structure for Model Checking Quantum Circuits

We define a Kripke structure $K = \langle S, I, T, A, L \rangle$ to conduct model checking for quantum circuits. Our formalization can be used as a general framework to formally specify and verify quantum circuits as follows:

- S and T can be reused for any quantum circuit.
- I is required to specify initial states.
- A and L are required to specify some desired properties for quantum circuits.

A Kripke Structure for Model Checking Quantum Circuits

Each state in S is expressed as $\{obs\}$, where obs is a soup of six distinct observable components as follows:

- (`mState`:ms) denotes the mixed quantum state ms.
- (`#qubits`:n) denotes the number of qubits n.
- (`bits`:bm) denotes the classical bits obtained from measurements and stored in a bit map bm.
- (`prob`:p) denotes the probability p at the current quantum state.
- (`actions`:al) denotes the action list al, guiding us on how the circuit works.
- (`isEnd`:b) denotes termination with Boolean flag b.

A Kripke Structure for Model Checking Quantum Circuits

The state transitions in T for quantum circuits are formalized as follows:

```
--- unitary evolution
crl [U] : {(mState: MS) (actions: (A AL)) (#qubits: N) OCs}
=> {(mState: MS') (actions: AL) (#qubits: N) OCs}
if isBasicAction(A) /\ MS' := unitary(MS, A, N) .
--- measurement
crl [M0] : {(mState: MS) (actions: (M(N') AL)) (prob: Prob) (bits:
    BM) (#qubits: N) OCs}
=> {(mState: MS') (actions: AL) (prob: (Prob .* Prob')) (bits:
    insert(N', 0, BM)) (#qubits: N) OCs}
if {mState: MS', prob: Prob'} := measure(MS, N, P0, N') .
crl [M1] : {(mState: MS) (actions: (M(N') AL)) (prob: Prob) (bits:
    BM) (#qubits: N) OCs}
=> {(mState: MS') (actions: AL) (prob: (Prob .* Prob')) (bits:
    insert(N', 1, BM)) (#qubits: N) OCs}
if {mState: MS', prob: Prob'} := measure(MS, N, P1, N') .
```

A Kripke Structure for Model Checking Quantum Circuits

```
--- conditional gates
rl [cif] : {(qstate: Q) (bits: ((N |-> N1),BM)) (actions: ((c[N] ==
   N2 ? AL’) AL)) OCs}
=> {(qstate: Q) (bits: ((N |-> N1), BM))
    (actions: ((if (N1 == N2) then AL’ else nil fi) AL)) OCs} .
--- termination
rl [end] : {(actions: nil) (isEnd: false) OCs}
=> {(actions: nil) (isEnd: true) OCs} .
--- to make T total
rl [stutter]: {(isEnd: true) OCs} => {(isEnd: true) OCs} .
```

Contents

Model Checking Quantum Teleporation

- The initial state for Quantum Teleportation (QT)

```
init = {(isEnd: false)
(#qubits: findN(ES))
(mState: convert(ES))
(prob: 1)
(bits: empty)
(actions: H(1) CX(1, 2) CX(0, 1) H(0)
          M(0) M(1)
          c[1] == 1 ? X(2)
          c[0] == 1 ? Z(2))}
```

where ES represents `{(a.|0>+b.|1>)(x)|0>(x)|0>,1}`, the two functions `findN(_)` and `convert(_)` are to calculate the number of qubits and the density operator of a mixed state from a given ensemble ES.

- $I_{QT} = \{\texttt{init}\}$

Model Checking Quantum Teleporation

- A_{QT} consists of an atomic proposition `isSuccess`
- L_{QT} is defined:

```
eq {(isEnd: true) (mState: MS) (prob: Prob) (#qubits: N) OCs} |=
    isSuccess
= Prob > 0 implies
  tr[1]((tr[0](MS, N)), N) == (I (x) I (x) (PSI x (PSI)^+)) .
eq {OCs} |= PROP = false [owise] .
```

  where `PSI` is the input state of the protocol being transferred and the function `tr[_](_,_)` works as the partial trace over a sub-system.

- $K_{QT} \models \texttt{True}\ \mathcal{U}\ \texttt{isSuccess}$

```
modelCheck(init, True U isSuccess)
```

A Support Tool and Experimental Results

- A support tool implemented in Maude for handling mixed states is extended from our previous support tool for pure states[5].
- The implementation is available at `https://github.com/canhminhdo/QTC-Maude`

Protocol	Qubits	States	Pure States Rewrite Steps	Pure States Time	Mixed States Rewrite Steps	Mixed States Time
Superdense Coding	2	9	685	$\approx$ 0ms	2,088	2ms
Quantum Teleportation	3	27	4,340	3ms	29,095	30ms
Quantum Secret Sharing	4	65	16,449	9ms	211,831	519ms
Entanglement Swapping	4	33	6,930	4ms	56,193	40ms

[5] Do and Ogata, "Symbolic Model Checking Quantum Circuits in Maude".

Contents

Conclusions and Future Work

- We have extended our symbolic approach to handle mixed states using density operators and have developed a support tool in Maude.
- Several quantum communication protocols have been successfully verified using our approach/support tool.
- As one piece of future work, we would conduct more case studies in which the statistical mixture of multiple pure states is realistically presented.

Thank You!