上海市高可信计算重点实验室
Shanghai Key Laboratory of Trustworthy Computing

Formal Verification of Quantum Protocols

Yuxin Deng

East China Normal University

1. X. Qin, Y. Deng, and W. Du. Verifying Quantum Communication Protocols with Ground Bisimulation. TACAS'20, LNCS 12079, pages 21-38. Springer, 2020.
2. W. Shi, Q. Cao, Y. Deng, H. Jiang, Y. Feng. Symbolic Reasoning about Quantum Circuits in Coq. Journal of Computer Science and Technology 36(6):1291-1306, 2021.

Outline

Part I: Verification via ground bisimulation

- Preliminaries
- Quantum bisimulation
- Algorithm for checking ground bisimulation
- Implementation and experiments
- Summary

Part II: Verification via Coq

- Background
- Symbolic reasoning
- Experiments
- Summary

Part I: Verification via ground bisimulation

Correctness of protocols or algorithms

SPECIFICATION $\sim$ IMPLEMENTATION

$$Alice \stackrel{def}{=} \underline{c}_A?q_2.CN[q_1,q_2].H[q_1].M[q_1,q_2;x].Set^{\Psi}[q_1,q_2].e!x.\mathbf{nil};$$

$$Bob \stackrel{def}{=} \underline{c}_B?q_3.e?x.\sum_{0\leq i\leq 3}(\mathbf{if}\ x=i\ \mathbf{then}\ \sigma^i[q_3].\mathbf{nil});$$

$$EPR \stackrel{def}{=} Set^{\Psi}[q_1,q_2].\underline{c}_A!q_2.\underline{c}_B!q_3.\mathbf{nil};$$

$$Tel_{spec} \stackrel{def}{=} SWAP[q_1,q_3].\mathbf{nil}.$$

$$Tel \stackrel{def}{=} (Alice||Bob||EPR)\setminus\{\underline{c}_A,\underline{c}_B,e\}$$

Labelled transition systems

Def. A *labelled transition system* (LTS) is a triple $\langle S, Act, \rightarrow \rangle$, where

1. S is a set of states
2. Act is a set of actions
3. $\rightarrow \ \subseteq \ S \times Act \times S$ is the transition relation

Write $s \xrightarrow{\alpha} s'$ for $(s, \alpha, s') \in \rightarrow$.

Bisimulation

$$\begin{array}{ccc} s & \xrightarrow{a} & s' \\ \mathcal{R} & & \mathcal{R} \\ t & \xrightarrow{a} & t' \end{array}$$

s and t are bisimilar if there exists a bisimulation $\mathcal{R}$ with $s \; \mathcal{R} \; t$.

[Park, 1981], [Milner, 1989]

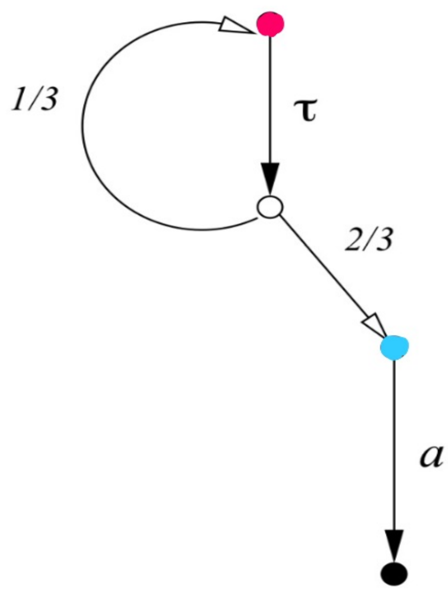
Probabilistic labelled transition systems

Def. A *probabilistic labelled transition system* (pLTS) is a triple $\langle S, Act, \rightarrow \rangle$, where

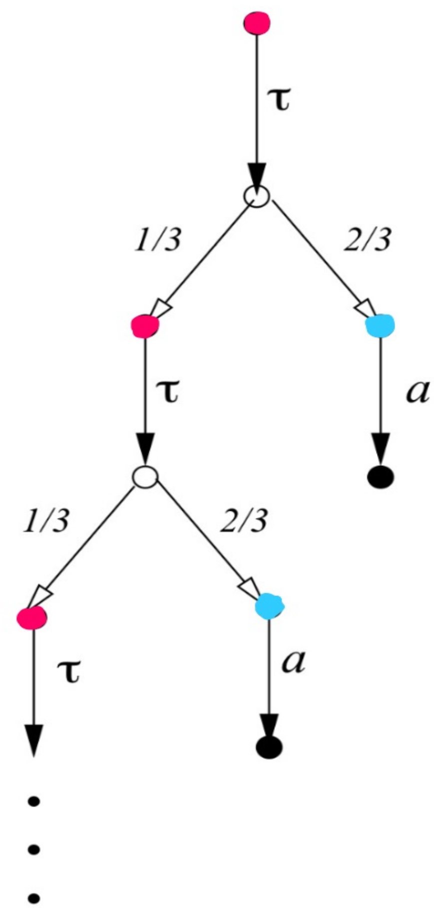
1. S is a set of states
2. Act is a set of actions
3. $\rightarrow \;\subseteq\; S \times Act \times \mathcal{D}(S)$.

We usually write $s \xrightarrow{\alpha} \Delta$ in place of $(s, \alpha, \Delta) \in \rightarrow$.

Example



(a)



(b)

State-based probabilistic bisimulation

$$\begin{array}{ccc} s & \xrightarrow{a} & \Delta \\ \mathcal{R} & & \mathcal{R}^{\circ} \\ t & \xrightarrow{a} & \Theta \end{array}$$

Write $\sim_s$ for the largest state-based probabilistic bisimilarity.

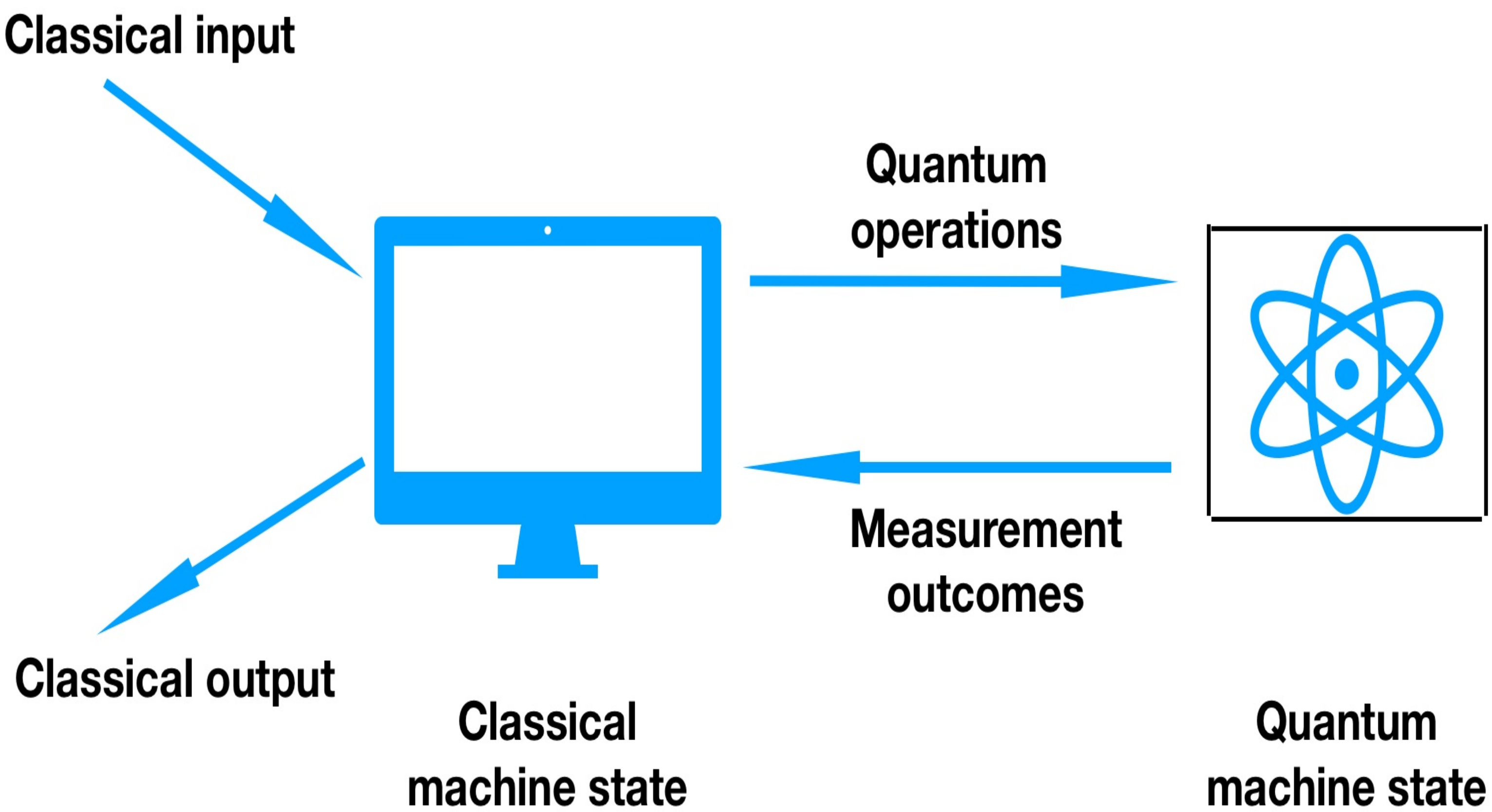
Lifting relations

Def. Let S, T be two countable sets and $\mathcal{R} \subseteq S \times T$ be a binary relation. The lifted relation $\mathcal{R}^\circ \subseteq \mathcal{D}(S) \times \mathcal{D}(T)$ is the smallest relation satisfying

1. $s \; \mathcal{R} \; t$ implies $\overline{s} \; \mathcal{R}^\circ \; \overline{t}$
2. $\Delta_i \mathcal{R}^\circ \Theta_i$ for all $i \in I$ implies $(\sum_{i \in I} p_i \cdot \Delta_i) \; \mathcal{R}^\circ \; (\sum_{i \in I} p_i \cdot \Theta_i)$, where $\sum_i p_i = 1$.

[D. et al., CONCUR 2009]

Hybrid architecture for quantum computation



The quantum process algebra qCCS

$$\begin{aligned} P, Q \quad ::= \quad & \mathbf{nil} \mid \tau.P \mid c?x.P \mid c!e.P \mid \underline{c}?q.P \mid \underline{c}!q.P \mid \mathcal{E}[\tilde{q}].P \mid M[\tilde{q}; x].P \mid \\ & P + Q \mid P \parallel Q \mid P[f] \mid P \backslash L \mid \mathbf{if}\ b\ \mathbf{then}\ P \mid A(\tilde{q}; \tilde{x}) \end{aligned}$$

Operational semantics

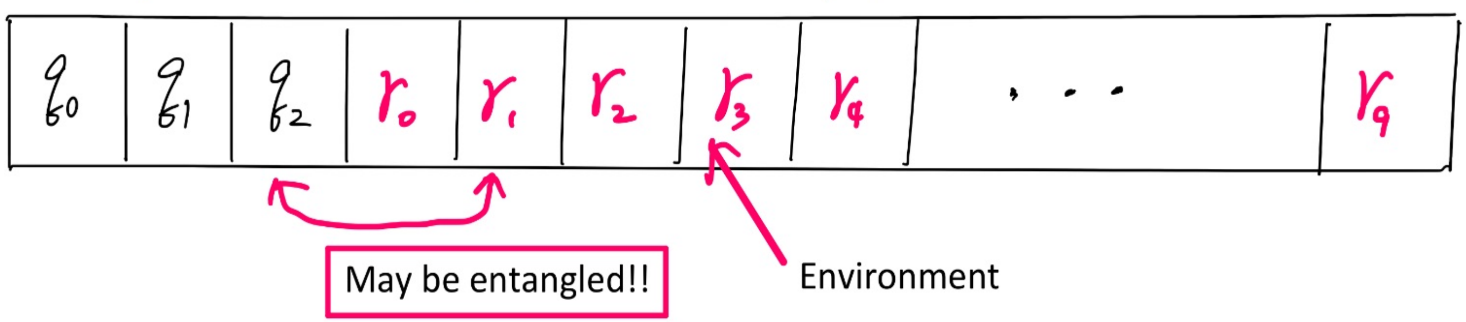
Let P be a closed quantum process. A pair of the form

$$\langle P, \rho \rangle$$

is called a configuration, where ρ is a density operator. Let Con be the set of configurations, ranged over by $\mathcal{C}, \mathcal{D}, \ldots$.

$$\langle P, \rho \rangle$$

$$P = CNOT[q_0, q_1].M[q_1, q_2; x].nil$$



Operational semantics

Let $\mathcal{D}(Con)$, ranged over by $\mu, \nu, \cdots$, be the set of all finite-supported probabilistic distributions over Con. The operational semantics of qCCS is given by the pLTS $\langle Con, Act_c, \rightarrow\rangle$, where $\rightarrow \subseteq Con \times Act_c \times \mathcal{D}(Con)$ is the smallest relation satisfying some inference rules.

Operational semantics

(Oper)

$$\langle \mathcal{E}[\tilde{q}].P, \rho \rangle \xrightarrow{\tau} \langle P, \mathcal{E}_{\tilde{q}}(\rho) \rangle$$

(Meas)

$$\frac{M = \sum_{i \in I} \lambda_i E^i \qquad p_i = tr(E^i_{\tilde{q}} \rho)}{\langle M[\widetilde{q}; x].P, \rho \rangle \xrightarrow{\tau} \sum_{i \in I} p_i \langle P[\lambda_i / x], E^i_{\widetilde{q}} \rho E^i_{\widetilde{q}} / p_i \rangle}$$

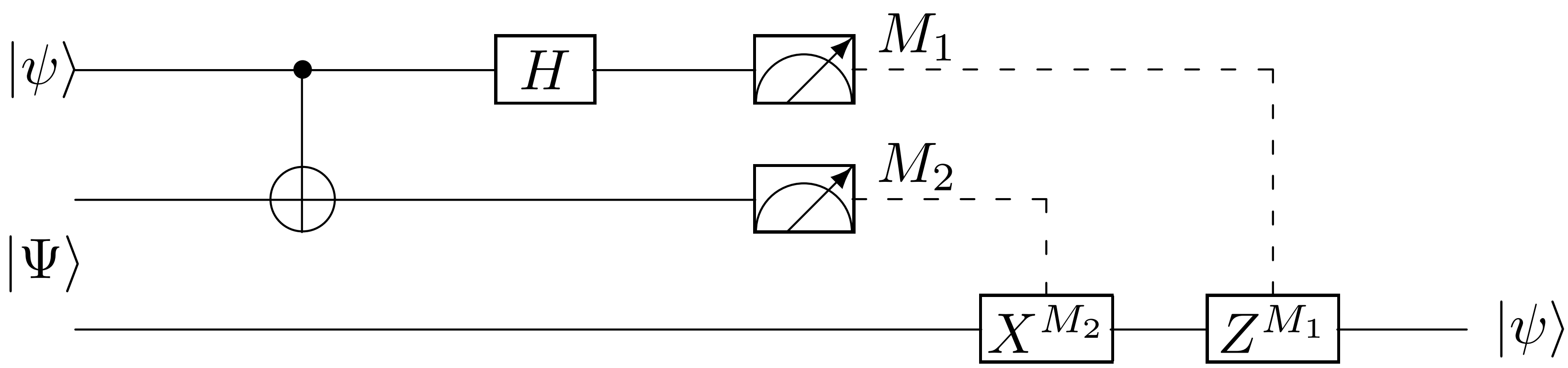
Here we consider projective measurements.

An example: Teleportation

Quantum teleportation [Bennett et al., PRL 1993] is one of the most important protocols in quantum information theory which makes use of a maximally entangled state to teleport an unknown quantum state by sending only *classical* information.

It serves as a key ingredient in many other quantum communication protocols.

An example: Teleportation



Let

$$
\begin{aligned}
Alice &:= CNot[q, q_1].H[q].M[q, q_1; x].c!x.\mathbf{nil} \\
Bob &:= c?x.U_x[q_2].\mathbf{nil} \\
Telep &:= (Alice \| Bob)\backslash\{c\}
\end{aligned}
$$

Here $M = \sum_{i=0}^{3} \lambda_i |\tilde{i}\rangle\langle\tilde{i}|$, and

$$
\begin{aligned}
U_x[q_2].\mathbf{nil} &:= \mathbf{if}\ x = \lambda_0\ \mathbf{then}\ \sigma_0[q_2].\mathbf{nil}\ +\ \mathbf{if}\ x = \lambda_1\ \mathbf{then}\ \sigma_1[q_2].\mathbf{nil} \\
&+\ \mathbf{if}\ x = \lambda_2\ \mathbf{then}\ \sigma_3[q_2].\mathbf{nil}\ +\ \mathbf{if}\ x = \lambda_3\ \mathbf{then}\ \sigma_2[q_2].\mathbf{nil}.
\end{aligned}
$$

An example: Teleportation

$$\langle Telep,\ [(\alpha|0\rangle+\beta|1\rangle)\otimes\tfrac{1}{\sqrt{2}}(|00\rangle+|11\rangle)]\rangle$$

$$\downarrow \tau$$

$$\langle (H[q].M[q,q_1;x].c!x.\mathbf{nil}\|Bob)\backslash\{c\},\ [\tfrac{1}{\sqrt{2}}(\alpha(|000\rangle+|011\rangle)+\beta(|110\rangle+|101\rangle))]\rangle$$

$$\downarrow \tau$$

$$\langle (M[q,q_1;x].c!x.\mathbf{nil}\|Bob)\backslash\{c\},\ [\tfrac{1}{2}(\alpha(|000\rangle+|100\rangle+|011\rangle+|111\rangle)+\beta(|010\rangle-|110\rangle+|001\rangle-|101\rangle))]\rangle$$

$$\downarrow \tau$$

1/4:

$$\langle (c!\lambda_0.\mathbf{nil}\|Bob)\backslash\{c\},\ [\alpha|000\rangle+\beta|001\rangle]\rangle \xrightarrow{\tau} \langle (\mathbf{nil}\|\sigma_0[q_2].\mathbf{nil})\backslash\{c\},\ [|00\rangle\otimes(\alpha|0\rangle+\beta|1\rangle)]\rangle \xrightarrow{\tau} \langle (\mathbf{nil}\|\mathbf{nil})\backslash\{c\},\ [|00\rangle\otimes(\alpha|0\rangle+\beta|1\rangle)]\rangle$$

1/4:

$$\langle (c!\lambda_1.\mathbf{nil}\|Bob)\backslash\{c\},\ [\alpha|011\rangle+\beta|010\rangle]\rangle \xrightarrow{\tau} \langle (\mathbf{nil}\|\sigma_1[q_2].\mathbf{nil})\backslash\{c\},\ [|01\rangle\otimes(\alpha|1\rangle+\beta|0\rangle)]\rangle \xrightarrow{\tau} \langle (\mathbf{nil}\|\mathbf{nil})\backslash\{c\},\ [|01\rangle\otimes(\alpha|0\rangle+\beta|1\rangle)]\rangle$$

1/4:

$$\langle (c!\lambda_2.\mathbf{nil}\|Bob)\backslash\{c\},\ [\alpha|100\rangle-\beta|101\rangle]\rangle \xrightarrow{\tau} \langle (\mathbf{nil}\|\sigma_3[q_2].\mathbf{nil})\backslash\{c\},\ [|10\rangle\otimes(\alpha|0\rangle-\beta|1\rangle)]\rangle \xrightarrow{\tau} \langle (\mathbf{nil}\|\mathbf{nil})\backslash\{c\},\ [|10\rangle\otimes(\alpha|0\rangle+\beta|1\rangle)]\rangle$$

1/4:

$$\langle (c!\lambda_3.\mathbf{nil}\|Bob)\backslash\{c\},\ [\alpha|111\rangle-\beta|110\rangle]\rangle \xrightarrow{\tau} \langle (\mathbf{nil}\|\sigma_2[q_2].\mathbf{nil})\backslash\{c\},\ [|11\rangle\otimes(\alpha|1\rangle-\beta|0\rangle)]\rangle \xrightarrow{\tau} \langle (\mathbf{nil}\|\mathbf{nil})\backslash\{c\},\ [|11\rangle\otimes(\alpha|0\rangle+\beta|1\rangle)]\rangle$$

Quantum ground bisimulation

Def. $\mathcal{R} \subseteq Con \times Con$ is a ground simulation if $\mathcal{C}\ \mathcal{R}\ \mathcal{D}$ implies that $qv(\mathcal{C}) = qv(\mathcal{D})$, $tr_{qv(P)}(\mathcal{C}) = tr_{qv(Q)}(\mathcal{D})$, and

whenever $\mathcal{C} \xrightarrow{\alpha} \Delta$, there is some distribution Θ with $\mathcal{D} \stackrel{\hat{\alpha}}{\Longrightarrow} \Theta$ and $\Delta \mathcal{R}^{\circ} \Theta$.

$\mathcal{R}$ is a ground bisimulation if both $\mathcal{R}$ and $\mathcal{R}^{-1}$ are ground simulations

Intuition

Two configurations are not bisimilar in 3 cases:

- they do not have the same set of free quantum variables for their processes;
- the density operators of them corresponding to their quantum registers are different;
- one configuration has a transition that cannot be matched by any possible weak combined transition from the other.

Intuition

Two configurations are not bisimilar in 3 cases:

- they do not have the same set of free quantum variables for their processes;
- the density operators of them corresponding to their quantum registers are different;
- one configuration has a transition that cannot be matched by any possible weak combined transition from the other
  $\longrightarrow$ reduced to a linear programming problem

Predicate LP

Use the algorithm of [Turrini and Hermanns 2015] to check the step condition.

- Add more edges and vertexes to construct a flow network;
- Generate constraints according to the flow network to reduce the problem into a linear programming problem.

We define a predicate **LP** which is true if and only if the linear programming problem has a solution.

A. Turrini and H. Hermanns, Polynomial time decision algorithms for probabilistic automata, Inf. & Comp. 244 (2015), 134-171.

The Algorithm

Require: Two pLTSs with initial configurations t and u.

Ensure: A boolean value b_{res} indicating if the two pLTSs are ground bisimilar.

function GroundBisimulation(t, u) =

  $NonBisim := \emptyset$

  function Bisim(t, u) = **try** $\{$

  $Bisim := \emptyset$

  $Visited := \emptyset$

  $Assumed := \emptyset$

  return Match$(t, u, Visited)$

  $\}$ **catch WrongAssumptionException** $\Rightarrow$ **Bisim**(t, u)

$Visited := Visited \cup \{(t,u)\}$ $\triangleright\ t = \langle P, \rho \rangle$ *and* $u = \langle Q, \sigma \rangle$

$b := \bigwedge_{\alpha \in Act(t)}$ **MatchAction**$(\alpha, t, u, Visited)$

$\overline{b} := \bigwedge_{\alpha \in Act(u)}$ **MatchAction**$(\alpha, u, t, Visited)$

$b_{c_1} := qv(P) = qv(Q)$

$b_{c_2} := tr_{qv(P)}(\rho) = tr_{qv(P)}(\sigma)$

$b_{res} := b \wedge \overline{b} \wedge b_{c_1} \wedge b_{c_2}$

if b_{res} is **tt then** $Bisim = Bisim \cup \{(t,u)\}$

else if b_{res} is **ff then**

    $NonBisim = NonBisim \cup \{(t,u)\}$

    if $(t,u) \in Assumed$ **then**

        raise WrongAssumptionException

return b_{res}

Algorithm 3 **MatchAction**$(\alpha, t, u, Visited)$

switch α **do**

  case $c!$

    for $t \xrightarrow{c!e_i} \Delta_i$ **do**

      Assume $\{t_k\}_{t_k \in \lceil \Delta_i \rceil}$ and $\{u_j\}_{u \overset{c!e'_j}{\Longrightarrow} \Gamma \wedge e_i = e'_j \wedge u_j \in \lceil \Gamma \rceil}$

      $\mathcal{R} := \{(t_k, u_j) | \mathbf{Close}(t_k, u_j, Visited) = \mathbf{tt}\}$

      $\theta_i := \mathbf{LP}(\Delta_i, u, \alpha, \mathcal{R})$

  otherwise

    for $t \xrightarrow{\alpha} \Delta_i$ **do**

      Assume $\{t_k\}_{t_k \in \lceil \Delta_i \rceil}$ and $\{u_j\}_{u \overset{\alpha}{\Longrightarrow} \Gamma \wedge u_j \in \lceil \Gamma \rceil}$

      $\mathcal{R} := \{(t_k, u_j) | \mathbf{Close}(t_k, u_j, Visited) = \mathbf{tt}\}$

      $\theta_i := \mathbf{LP}(\Delta_i, u, \alpha, \mathcal{R})$

return $\bigwedge_i \theta_i$

Algorithm 4 Close

```
if (t, u) ∈ Bisim then
    return tt
else if (t, u) ∈ NonBisim then
    return ff
else if (t, u) ∈ Visited then
    Assumed = Assumed ∪ {(t, u)}
    return tt
else
    return Match(t, u, Visited))
```

Termination and Correctness

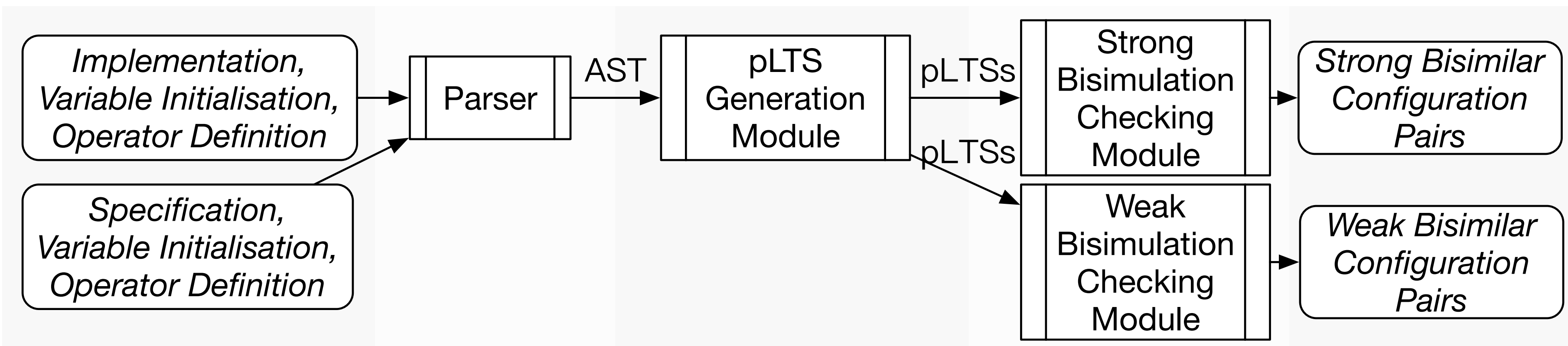
Thm. (Termination) Given two configurations t and u, the function **GroundBisimulation**(t, u) always terminates.

Thm. (Correctness) Given two configurations t and u from two pLTSs, **GroundBisimulation**(t, u) returns `true` if and only if they are ground bisimilar.

Thm. (Complexity) Let the number of nodes reachable from t and u be n. The time complexity of function **GroundBisimulation**(t, u) is polynomial in n.

Implementation

Verification workflow:



`https://github.com/MartianQXD/QBisim`

Experiments

Program	Variables	Bisi	Impl	Spec	N	B	ms
Super-dense coding	$q_1q_2 = \|00\rangle,\ x = 1$	Yes	16	5	9	20	712
	$q_1q_2 = \|00\rangle,\ x = 5$	No	6	2	-	-	54
Super-dense coding (modified)	$q_1q_2 = \|00\rangle,\ x = 5$	Yes	8	5	5	12	342
Teleportation	$q_1q_2q_3 = \|100\rangle$	Yes	34	3	22	22	910
	$q_1q_2q_3 = \frac{1}{\sqrt{2}}\|000\rangle + \frac{1}{\sqrt{2}}\|100\rangle$	Yes	34	3	22	22	923
	$q_1q_2q_3 = \frac{\sqrt{3}}{2}\|000\rangle + \frac{1}{2}\|100\rangle$	Yes	34	3	22	22	934
Secret Sharing	$q_1q_2q_3q_4 = \|1000\rangle$	Yes	103	3	65	65	5704
	$q_1q_2q_3q_4 = \frac{1}{\sqrt{2}}\|0000\rangle + \frac{1}{\sqrt{2}}\|1000\rangle$	Yes	103	3	65	65	5538
	$q_1q_2q_3q_4 = \frac{\sqrt{3}}{2}\|0000\rangle + \frac{1}{2}\|1000\rangle$	Yes	103	3	65	65	5485
BB84	$q_1q_2q_3 = \|000\rangle$	Yes	152	80	1084	3216	393407
B92	$q_1q_2 = \|00\rangle$	Yes	64	80	466	1284	105347
E91	$q_1q_2q_3q_4 = \|0000\rangle$	Yes	124	80	964	2676	334776

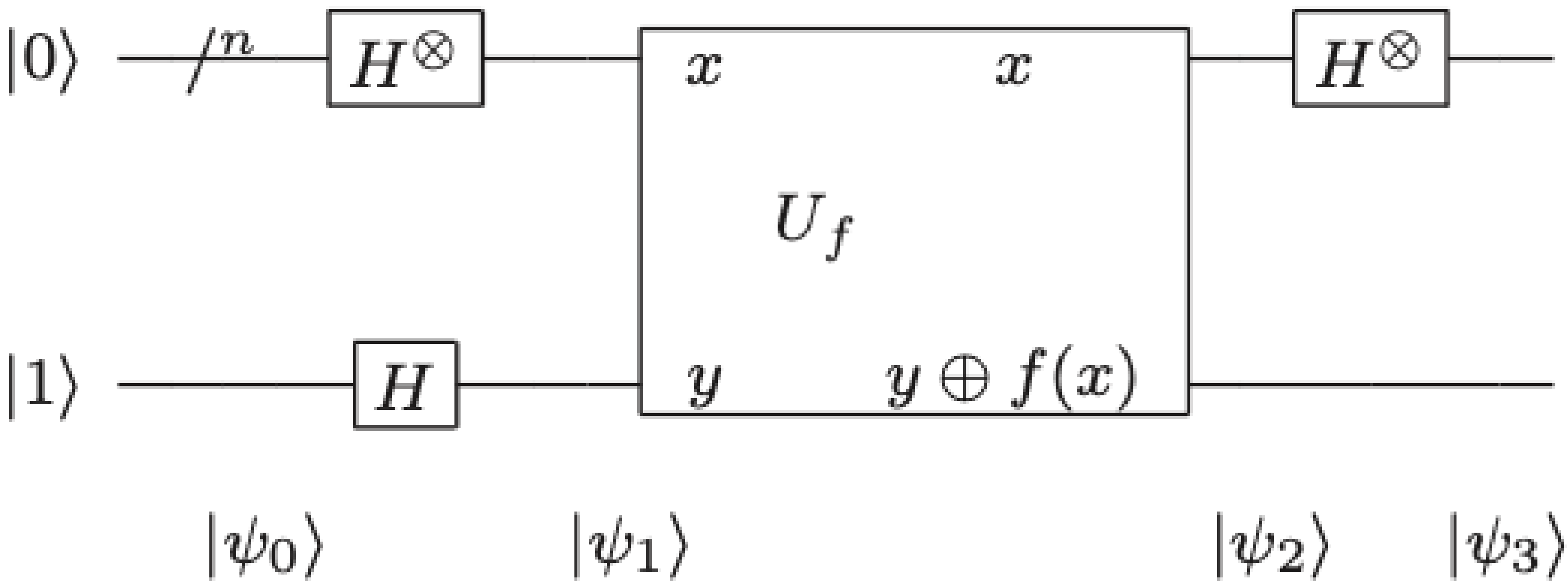
Summary

- An on-the-fly algorithm to check ground bisimulation for quantum processes in qCCS
- A tool to verify quantum communication protocols modelled as qCCS processes
- Verification of several non-trivial quantum communication protocols from super-dense coding to key distribution

Part II: Verification via Coq

Motivation

The Deutsch-Jozsa algorithm family: to determine if a function $f : \{0,1\}^n \to \{0,1\}$ is a constant or a balanced function.



Existing work

- Paykin et al. defined a quantum circuit language QWIRE in Coq
- Hietala et al. developed a quantum circuit compiler VOQC in Coq
- Liu et al. formalized a quantum Hoare logic in Isabelle/HOL
- Unruh developed a relational quantum Hoare logic in Isabelle/HOL
- Chareton et al. proposed a verification framework QBRICKS in Why3
- ...

Terms and laws

Scalars:	$\mathbb{C}$
Basic vectors:	$\|0\rangle$, $\|1\rangle$
Operators:	$\cdot, \times, +, \otimes, \dagger$
Laws:	**L1** $\langle 0\|0\rangle = \langle 1\|1\rangle = 1,\ \langle 0\|1\rangle = \langle 1\|0\rangle = 0$
	L2 Associativity of $\cdot,\ \times,\ +,\ \otimes$
	L3 $0 \cdot A_{m\times n} = \mathbf{0}_{m\times n},\ c\cdot \mathbf{0} = \mathbf{0},\ 1\cdot A = A$
	L4 $c\cdot(A+B) = c\cdot A + c\cdot B$
	L5 $c\cdot(A\times B) = (c\cdot A)\times B = A\times(c\cdot B)$
	L6 $c\cdot(A\otimes B) = (c\cdot A)\otimes B = A\otimes(c\cdot B)$
	L7 $\mathbf{0}_{m\times n}\times A_{n\times p} = \mathbf{0}_{m\times p} = A_{m\times n}\times \mathbf{0}_{n\times p}$
	L8 $I_m\times A_{m\times n} = A_{m\times n} = A_{m\times n}\times I_n,\ \ I_m\otimes I_n = I_{mn}$
	L9 $\mathbf{0}+A = A = A+\mathbf{0}$
	L10 $\mathbf{0}_{m\times n}\otimes A_{p\times q} = \mathbf{0}_{mp\times nq} = A_{p\times q}\otimes \mathbf{0}_{m\times n}$
	L11 $(A+B)\times C = A\times C + B\times C,\ C\times(A+B) = C\times A + C\times B$
	L12 $(A+B)\otimes C = A\otimes C + B\otimes C,\ C\otimes(A+B) = C\otimes A + C\otimes B$
	L13 $(A\otimes B)\times(C\otimes D) = (A\times C)\otimes(B\times D)$
	L14 $(c\cdot A)^\dagger = c^*\cdot A^\dagger,\ (A\times B)^\dagger = B^\dagger\times A^\dagger$
	L15 $(A+B)^\dagger = A^\dagger + B^\dagger,\ (A\otimes B)^\dagger = A^\dagger\otimes B^\dagger$
	L16 $(A^\dagger)^\dagger = A$

Reduction strategies

- orthogonal_reduce:

  $\langle 0|0\rangle = \langle 1|1\rangle,\ \langle 0|1\rangle = \langle 1|0\rangle = 0$

- base_reduce:

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

  $\mathbf{B_0} \times |0\rangle = |0\rangle \times \langle 0| \times |0\rangle = |0\rangle \times (\langle 0| \times |0\rangle) = |0\rangle \times 1 = |0\rangle$

- gate_reduce:

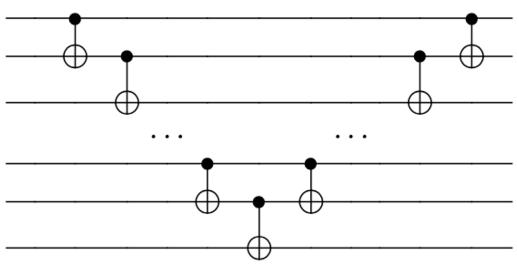
  $\mathbf{X} \times |0\rangle = (\mathbf{B_1} + \mathbf{B_2}) \times |0\rangle = \mathbf{B_1} \times |0\rangle + \mathbf{B_2} \times |0\rangle = 0 + |1\rangle = |1\rangle$

- operate_reduce:

  Puts together all the above results to reason about circuits.

Example: the U_f gate

```
Lemma DJ_1 :
    (n > 0)%nat ->
    (Uf n) × ((kron_n n |+⟩) ⊗ |-⟩) = (kron_n n |+⟩) ⊗ |-⟩.
```



$$
\begin{aligned}
& U_f^{k+1} \times (|+\rangle^{\otimes(k+1)} \otimes |-\rangle) \\
&= (CX \otimes I_{2^k}) \times (I_2 \otimes U_f^k) \times (CX \otimes I_{2^k}) \times (|+\rangle \otimes |+\rangle \otimes |+\rangle^{\otimes(k-1)} \otimes |-\rangle) \\
&= (CX \otimes I_{2^k}) \times (I_2 \otimes U_f^k) \times ((CX \otimes I_{2^k}) \times ((|+\rangle \otimes |+\rangle) \otimes (|+\rangle^{\otimes(k-1)} \otimes |-\rangle))) \\
&= (CX \otimes I_{2^k}) \times (I_2 \otimes U_f^k) \times ((CX \times (|+\rangle \otimes |+\rangle)) \otimes (I_{2^k} \times (|+\rangle^{\otimes(k-1)} \otimes |-\rangle))) \\
&= (CX \otimes I_{2^k}) \times ((I_2 \otimes U_f^k) \times ((|+\rangle \otimes |+\rangle) \otimes (|+\rangle^{\otimes(k-1)} \otimes |-\rangle))) \\
&= (CX \otimes I_{2^k}) \times ((I_2 \times |+\rangle) \otimes (U_f^k \times (|+\rangle^{\otimes k} \otimes |-\rangle))) \\
&= (CX \otimes I_{2^k}) \times (|+\rangle \otimes (|+\rangle^{\otimes k} \otimes |-\rangle)) \\
&= (CX \otimes I_{2^k}) \times ((|+\rangle \otimes |+\rangle) \otimes (|+\rangle^{\otimes k-1} \otimes |-\rangle)) \\
&= (CX \times (|+\rangle \otimes |+\rangle)) \otimes (I_{2^k} \times (|+\rangle^{\otimes k-1} \otimes |-\rangle)) \\
&= |+\rangle^{\otimes(k+1)} \otimes |-\rangle
\end{aligned}
$$

Circuit equivalences

- Matrix equivalence:

  Consider each quantum gate as a unitary matrix and the whole circuit as a composition of matrices.

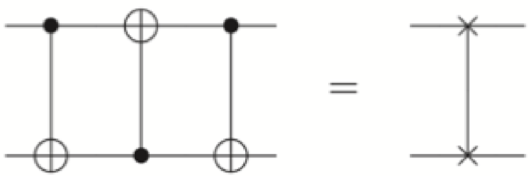
- Observational equivalence:

  Consider a circuit as an operator that changes input quantum states to output.

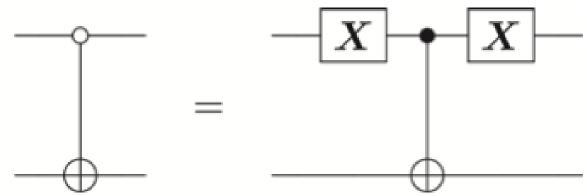
```
Lemma ObsEquiv_state: forall {n} (ψ ϕ: Matrix n 1),
  ψ ≈ ϕ <-> ψ × (ψ†) = ϕ × (ϕ†) .
```

```
Lemma ObsEquiv_operator: forall {n} (A B: Matrix n n),
  A ≈ B <-> (forall ψ: Matrix n 1, A × ψ ≈  B × ψ).
```

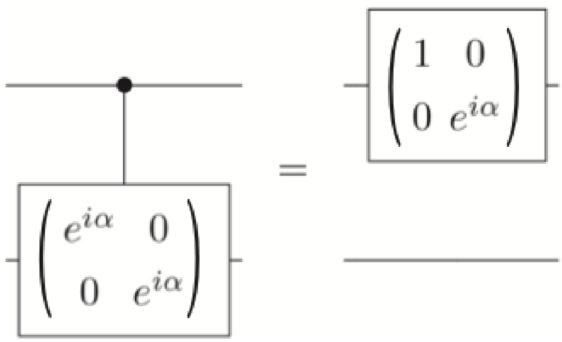
Circuit equivalences



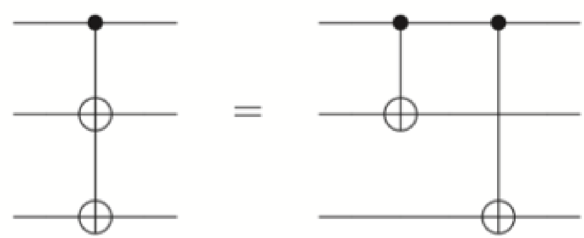
(a)



(b)



(c)



(d)

Summary

A symbolic approach to reasoning about quantum circuits in Coq based on a small set of equational laws.

Comparison with the computational approach.

	Deutsch	Simon	Teleportation	Secret sharing	QFT	Grover
Symbolic	3656	53795	39715	68919	25096	146834
Computational	25190	180724	46450	170490	68730	934570

Future work

- Check symbolic bisimulations
- Verify quantum protocols with more qubits
- Extend the symbolic approach from quantum circuit models to quantum programs

Y. Feng, Y. Deng, and M. Ying, Symbolic bisimulation for quantum processes, ACM Trans. Computational Logic 15 (2014), no. 2, 1–32.

Thank you!

yxdeng@sei.ecnu.edu.cn