An Algebraic Specification for Quantum Computation in Maude

Canh Minh Do Kazuhiro Ogata

{canhdo,ogata}@jaist.ac.jp

Japan Advanced Institute of Science and Technology (JAIST)

The 16th International Workshop on Rewriting Logic and Its Applications (WRLA 2026)
Torino, Italy - April 12, 2026

Contents

Contents

Introduction

- With the rapid advancement of quantum computing, formal verification of quantum systems has become an increasingly important research topic.
- The algebraic specification community, particularly the Maude community, has started to show interest in quantum computing.
- However, a dedicated algebraic specification for quantum computation is still lacking.
- This work presents |AS4QC>, an algebraic specification for quantum computation in Maude, which provides a formal framework for modeling, symbolic and exact reasoning about, and verifying quantum systems.

Contents

Hilbert Spaces

- A Hilbert space $\mathcal{H}$ serves as the state space of a quantum system that is a complete complex vector space equipped with an inner product.
- A qubit is a quantum system whose state space is the two-dimensional Hilbert space $\mathcal{H}_2 = \mathbb{C}^2$.
- A qubit $|\psi\rangle$ can be expressed as a superposition of $|0\rangle$ and $|1\rangle$ as follows:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = (\alpha, \beta)^T$$

  where $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$, and $\alpha, \beta \in \mathbb{C}$ such that $|\alpha|^2 + |\beta|^2 = 1$.
- The set $\{|0\rangle, |1\rangle\}$ forms an orthonormal basis of $\mathcal{H}_2$ and is called the computational basis.
- For multiple qubits, the tensor product $\mathcal{H}_A \otimes \mathcal{H}_B$ of Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ is defined as a vector space consisting of linear combinations of the product states

$$|\psi_1\psi_2\rangle = |\psi_1\rangle\,|\psi_2\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$$

  where $|\psi_1\rangle \in \mathcal{H}_A$ and $|\psi_2\rangle \in \mathcal{H}_B$.
- Any state in $\mathcal{H}_A \otimes \mathcal{H}_B$ cannot be written as a product state called an entangled state.

Unitary Transformation

- A unitary transformation on a Hilbert space $\mathcal{H}$ is a linear operator $U : \mathcal{H} \to \mathcal{H}$ satisfying $UU^\dagger = U^\dagger U = I_\mathcal{H}$, which deterministically changes a state $|\psi\rangle$ to $U|\psi\rangle$.
- 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:

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix},\ X = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix},\ Y = \begin{pmatrix}0 & -i\\ i & 0\end{pmatrix},\ Z = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix},\ T = \begin{pmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{pmatrix}.$$

- For example, we have

$$X|0\rangle = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix} = |1\rangle, \qquad H|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1\\ 0\end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle),$$
$$X|1\rangle = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}0\\ 1\end{pmatrix} = |0\rangle, \qquad H|1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0\\ 1\end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Unitary Transformation (cont.)

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

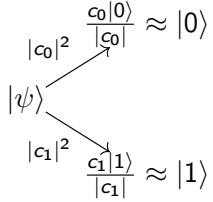
$$CX = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad SWAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

- For example, we have

$$\begin{aligned} CX\,|00\rangle &= |00\rangle, & SWAP\,|00\rangle &= |00\rangle, \\ CX\,|01\rangle &= |01\rangle, & SWAP\,|01\rangle &= |10\rangle, \\ CX\,|10\rangle &= |11\rangle, & SWAP\,|10\rangle &= |01\rangle, \\ CX\,|11\rangle &= |10\rangle, & SWAP\,|11\rangle &= |11\rangle. \end{aligned}$$

Measurement

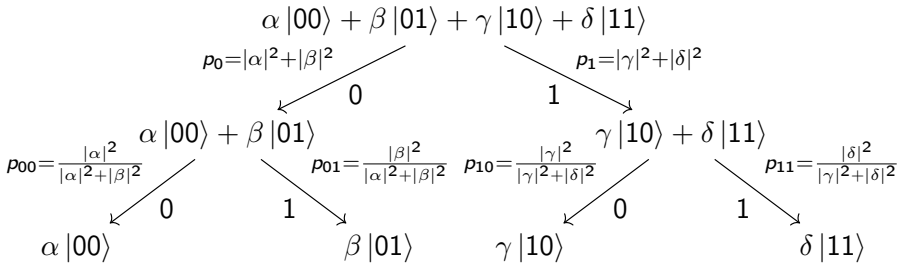
- A quantum measurement on a quantum system in the Hilbert space $\mathcal{H}$ is a collection of measurement operators $\{M_m\}$ satisfying the completeness relation $\sum_m M_m^\dagger M_m = I$.
- Measuring a state $|\psi\rangle$ yields outcome m with probability $p(m) = \| M_m |\psi\rangle \|^2$, and the state is changed to $|\psi_m\rangle = \frac{M_m|\psi\rangle}{\sqrt{p(m)}}$ nondeterministically.
- After executing the measurement $\{M_0 = |0\rangle\langle 0|, M_1 = |1\rangle\langle 1|\}$, a qubit $|\psi\rangle = c_0|0\rangle + c_1|1\rangle$ is collapsed into either $\frac{M_0|\psi\rangle}{|c_0|}$ with probability $|c_0|^2$ or into $\frac{M_1|\psi\rangle}{|c_1|}$ with probability $|c_1|^2$.



Normalization Convention

Convention 2.1 (Normalization Convention adopted from Selinger)

Each state is normalized so that the sum of the absolute squares of the amplitudes equals the total probability of reaching that state.



☞ Not normalizing the quantum state after each measurement significantly simplifies our representation and computation.

Projection

- For each closed subspace V of $\mathcal{H}$, there exists a unique projection operator $\mathcal{P}_V$.
- Every state $|\psi\rangle \in \mathcal{H}$ can be written as

$$|\psi\rangle = |\psi_V\rangle + |\psi_{V^\perp}\rangle$$

  with $|\psi_V\rangle \in V$ and $|\psi_{V^\perp}\rangle \in V^\perp$, the orthogonal complement of V.
- The projection $\mathcal{P}_V : \mathcal{H} \to V$ is defined by $\mathcal{P}_V |\psi\rangle = |\psi_V\rangle$.
- If a state $|\psi\rangle$ is in the closed subspace V of the projection operator $\mathcal{P}_V$, then

$$\mathcal{P}_V |\psi\rangle = |\psi\rangle .$$

Contents

Complex Number Representation

- Giles and Selinger proved that a unitary matrix can be exactly realized by a quantum circuit over the universal Clifford + T gate set, possibly using one additional ancilla, if and only if its matrix entries belong to the ring $\mathbb{D}[\omega]$.
- Therefore, we can use the ring $\mathbb{D}[\omega]$ to specify many standard quantum gates, including the universal Clifford + T gate set.
- This ring consists of all complex numbers of the form

$$\frac{1}{\sqrt{2}^k}(a + b\omega + c\omega^2 + d\omega^3)$$

  where $k \in \mathbb{N}, a, b, c, d \in \mathbb{Z}$, and $\omega = e^{i\pi/4} = \cos(\pi/4) + i\,\sin(\pi/4) = (1 + i)/\sqrt{2}$.
- Using the ring $\mathbb{D}[\omega]$, a complex number is algebraically represented by a quadruple (a, b, c, d) of integers and a normalization factor k of a natural number.

Complex Number Representation

- We assume that all amplitudes of a quantum state share a common normalization factor k because initial quantum states are usually basis states.
  - We store a single global value k for the whole quantum state and initially set it to zero.
  - For each application of an H, Rx[$\pi/2$], Ry[$\pi/2$], or Rz[$\pi/2$] gate, the value of k is incremented since these gates involve a factor of $1/\sqrt{2}$. Note that this factor is omitted in these quantum gates, making their representation simplified.
  - The final quantum state is normalized by multiplying $(1/\sqrt{2})^k$.
- Now each amplitude of a quantum state is represented as a quadruple (a, b, c, d) of integers, and a value k is stored globally.
- Addition and multiplication operations on complex numbers in this quadruple form are therefore significantly simplified.

Complex Number Representation

- We have the following lemma to distinguish between zero and nonzero complex numbers.

Lemma 1

Let $\frac{1}{\sqrt{2}^k}(a + b\omega + c\omega^2 + d\omega^3)$ be an element of the ring $\mathbb{D}[\omega]$, where $k \in \mathbb{N}$, $a, b, c, d \in \mathbb{Z}$, and $\omega = e^{i\pi/4}$. Then, we have

$$\frac{1}{\sqrt{2}^k}(a + b\omega + c\omega^2 + d\omega^3) = 0 \text{ if and only if } a = b = c = d = 0.$$

Proof.

It is straightforward to prove this lemma by substituting $\omega = (1 + i)/\sqrt{2}$, $\omega^2 = i$, and $\omega^3 = (i - 1)/\sqrt{2}$. □

Complex Number Representation

- We formalize the complex numbers as follows:

```
sorts ZeroCpx NzCpx Cpx .   subsorts ZeroCpx NzCpx < Cpx .
op (_,_,_,_) : Zero Zero Zero Zero -> ZeroCpx [ctor] .
op (_,_,_,_) : NzInt Int Int Int   -> NzCpx   [ctor] .
op (_,_,_,_) : Int NzInt Int Int   -> NzCpx   [ctor] .
op (_,_,_,_) : Int Int NzInt Int   -> NzCpx   [ctor] .
op (_,_,_,_) : Int Int Int NzInt   -> NzCpx   [ctor] .
op (_,_,_,_) : Int Int Int Int     -> Cpx     [ctor] .
op _+_ : Cpx Cpx     -> Cpx   [comm assoc prec 33] .
op _*_ : Cpx Cpx     -> Cpx   [comm assoc prec 31] .
op _*_ : NzCpx NzCpx -> NzCpx [ditto] .
op _^* : Cpx   -> Cpx   [prec 29] .
op _^* : NzCpx -> NzCpx [prec 29] .
op _^* : NzCpx -> NzCpx [prec 29] .
```

Complex Number Representation

- The conjugate $(a + b\omega + c\omega^2 + d\omega^3)^*$ is $(a - d\omega - c\omega^2 - a\omega^3)$. Then, we formalize

  ```
  eq (I1, I2, I3, I4)^* = (I1, - I4, - I3, - I2) .
  ```

  where `I1`, `I2`, `I3`, `I4` are variables of sort `Int`.
- We have the following result to facilitate the calculation of the probability of a basis state.

$$\begin{aligned} |a + b\omega + c\omega^2 + d\omega^3|^2 &= (a + b\omega + c\omega^2 + d\omega^3)(a + b\omega + c\omega^2 + d\omega^3)^* \\ &= (a + b\omega + c\omega^2 + d\omega^3)(a - d\omega - c\omega^2 - a\omega^3) \\ &= a^2 + b^2 + c^2 + d^2 + \sqrt{2}(ab + bc + cd - ad). \end{aligned}$$

Note that the value of the probability is a real number when $\sqrt{2}$ appears in the result.

Complex Number Representation

- We currently support X, Y, Z, H, S, T, Rx[$\pi/2$], Ry[$\pi/2$], Rz[$\pi/2$], CX, CY, CZ, SWAP, CCX, CCY, CCZ, MCX, MCY, MCZ, MCSWAP, which already includes the universal Clifford + T gate set.
- Form example,

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \longrightarrow H = \begin{pmatrix}(1,0,0,0) & (1,0,0,0)\\ (1,0,0,0) & (-1,0,0,0)\end{pmatrix}.$$

$$Y = \begin{pmatrix}0 & -i\\ i & 0\end{pmatrix} \longrightarrow Y = \begin{pmatrix}(0,0,0,0) & (0,0,-1,0)\\ (0,0,1,0) & (0,0,0,0)\end{pmatrix}.$$

$$T = \begin{pmatrix}1 & 0\\ 0 & e^{i\pi/4}\end{pmatrix} \longrightarrow T = \begin{pmatrix}(1,0,0,0) & (0,0,0,0)\\ (0,0,1,0) & (0,0,0,0)\end{pmatrix}.$$

$$Rx[\pi/2] = \begin{pmatrix}0 & -i\\ -1 & 0\end{pmatrix} \longrightarrow Rx[\pi/2] = \begin{pmatrix}(0,0,0,0) & (0,0,-1,0)\\ (0,0,-1,0) & (0,0,0,0)\end{pmatrix}.$$

Quantum States and Quantum Operations

- We use Dirac notation to formalize quantum states and quantum operations.
- We first formalize basic vectors, covectors, and matrices written in Dirac notation as $|0\rangle$ and $|1\rangle$, $\langle 0|$ and $\langle 1|$, and $|0\rangle\langle 0|$, $|0\rangle\langle 1|$, $|1\rangle\langle 0|$, and $|1\rangle\langle 1|$, respectively.
- For each of vectors, covectors, and matrices, we formalize constructors of scalar multiplication $\cdot$, addition $+$, multiplication $\times$, tensor product $\otimes$, conjugate transpose †.
- We also formalize the inner product $\langle \_ | \_ \rangle$ and norm square $\| \_ \|^2$ operations for vectors
- Terms representing quantum states and quantum operations are then built from complex numbers, basic elements, and their constructors.

Quantum States

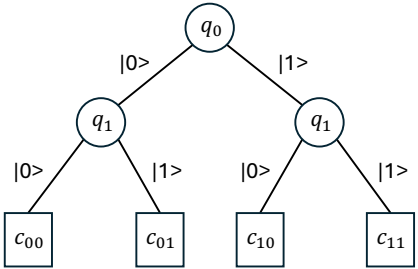


Figure: The binary decision tree of $c_{00}\,|00\rangle + c_{01}\,|01\rangle + c_{10}\,|10\rangle + c_{11}\,|11\rangle$

- We use a binary decision tree-based representation to enable more efficient manipulation for quantum states.

$$|0\rangle \otimes (c_{00} \cdot |0\rangle + c_{01} \cdot |1\rangle) + |1\rangle \otimes (c_{10} \cdot |0\rangle + c_{11} \cdot |1\rangle)$$

Quantum Operations

- We prepare quantum operations in a designated representation to speed up computation when applying them to quantum states.
- For example, we have the representations of some standard operations.

$$
\begin{array}{lcllcl}
\mathrm{X} & = & |0\rangle\langle 1| + |1\rangle\langle 0|\,, & \mathrm{Y} & = & (0,0,-1,0)\cdot|0\rangle\langle 1| + (0,0,1,0)\cdot|1\rangle\langle 0|\,, \\
\mathrm{Z} & = & |0\rangle\langle 0| + (-1,0,0,0)\cdot|1\rangle\langle 1|\,, & \mathrm{H} & = & |0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + (-1,0,0,0)\cdot|1\rangle\langle 1|\,, \\
\mathrm{CX} & = & |0\rangle\langle 0| \otimes \mathrm{I} + |1\rangle\langle 1| \otimes \mathrm{X}, & \mathrm{T} & = & |0\rangle\langle 0| + (0,1,0,0)\cdot|1\rangle\langle 1|\,, \\
\mathrm{P0} & = & |0\rangle\langle 0|\,, & \mathrm{P1} & = & |1\rangle\langle 1|\,,
\end{array}
$$

  where the factor $1/\sqrt{2}$ is omitted in the Hadamard gate H.
- The ring $\mathbb{D}[\omega]$ again simplifies the representation of these quantum operations, especially in the cases of H and T gates.

Automated Reasoning for Quantum Computation

- We leverage a set of laws from quantum mechanics and basic matrix operations to enable automated reasoning for quantum computation.

No.	Law
L1	$\langle 0\|0\rangle = \langle 1\|1\rangle = 1, \langle 0\|1\rangle = \langle 1\|0\rangle = 0$
L2	Associativity of $\times, +, \otimes$ and Commutativity of $+$
L3	$0 \cdot \boldsymbol{A}_{m\times n} = \mathbf{O}_{m\times n},\ c \cdot \mathbf{O} = \mathbf{O},\ 1 \cdot \boldsymbol{A} = \boldsymbol{A}$
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	$\mathbf{O}_{m\times n} \times \boldsymbol{A}_{n\times p} = \boldsymbol{A}_{m\times n} \times \mathbf{O}_{n\times p} = \mathbf{O}_{m\times p}$
L11	$\boldsymbol{I}_m \times \boldsymbol{A}_{m\times n} = \boldsymbol{A}_{m\times n} \times \boldsymbol{I}_n = \boldsymbol{A}_{m\times n}$
L12	$\boldsymbol{A} + \mathbf{O} = \mathbf{O} + \boldsymbol{A} = \mathbf{O}$
L13	$\mathbf{O}_{m\times n} \otimes \boldsymbol{A}_{p\times q} = \boldsymbol{A}_{p\times q} \otimes \mathbf{O}_{m\times n} = \mathbf{O}_{mp\times nq}$
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	$\|0\rangle^\dagger = \langle 0\|,\ \langle 0|^\dagger = |0\rangle,\ \|1\rangle^\dagger = \langle 1\|,\ \langle 1|^\dagger = |1\rangle$

Automated Reasoning for Quantum Computation

$$
\begin{aligned}
&\mathrm{H} \times |0\rangle \\
&\to (|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + (-1,0,0,0) \cdot |1\rangle\langle 1|) \times |0\rangle \\
&\to |0\rangle\langle 0| \times |0\rangle + |0\rangle\langle 1| \times |0\rangle + |1\rangle\langle 0| \times |0\rangle + ((-1,0,0,0) \cdot |1\rangle\langle 1|) \times |0\rangle \\
&\to |0\rangle + |1\rangle
\end{aligned}
$$

$$
\begin{aligned}
&(\mathrm{H} \otimes \mathrm{I}) \times (|0\rangle \otimes |0\rangle) \\
&\to (\mathrm{H} \times |0\rangle) \otimes (\mathrm{I} \times |0\rangle) \\
&\to (|0\rangle + |1\rangle) \otimes |0\rangle \\
&\to |0\rangle \otimes |0\rangle + |1\rangle \otimes |0\rangle
\end{aligned}
$$

$$
\begin{aligned}
&\mathrm{CX} \times ((\mathrm{H} \otimes \mathrm{I}) \times (|0\rangle \otimes |0\rangle)) \\
&\to (|0\rangle\langle 0| \otimes \mathrm{I} + |1\rangle\langle 1| \otimes \mathrm{X}) \times (|0\rangle \otimes |0\rangle + |1\rangle \otimes |0\rangle) \\
&\to (|0\rangle\langle 0| \otimes \mathrm{I} \times |0\rangle \otimes |0\rangle) + (|0\rangle\langle 0| \otimes \mathrm{I} \times |1\rangle \otimes |0\rangle) + (|1\rangle\langle 1| \otimes \mathrm{X} \times |0\rangle \otimes |0\rangle) + (|1\rangle\langle 1| \otimes \mathrm{X} \times |1\rangle \otimes |0\rangle) \\
&\to |0\rangle \otimes (\mathrm{I} \times |0\rangle) + |1\rangle \otimes (\mathrm{X} \times |0\rangle) \\
&\to |0\rangle \otimes |0\rangle + |1\rangle \otimes ((|1\rangle\langle 0| + |0\rangle\langle 1|) \times |0\rangle) \\
&\to |0\rangle \otimes |0\rangle + |1\rangle \otimes (|1\rangle\langle 0| \times |0\rangle + |0\rangle\langle 1| \times |0\rangle) \\
&\to |0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle
\end{aligned}
$$

Contents

Verification of Quantum Teleportation in |AS4QC>

```
fmod TELEPORT is
  pr QC .
  ops a b  : -> NzCpx .
  op |psi> : -> Vect  .
  eq |psi> = a . |0> + b . |1> .
  eq  a * a ^* + b * b ^*
  = (1,0,0,0) .
endfm
```

```
red analyze([
  H(1) CX(1,2) CX(0,1) H(0)
  (P0(1) U (P1(1) X(2)))
  (P0(0) U (P1(0) Z(2))),
  |psi> (x) |0> (x) |0>
]) .
```

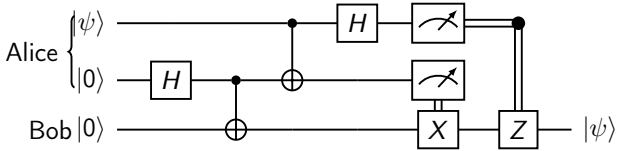


Figure: Quantum Teleportation

Output:

```
[|0>(x)|0>(x)(a.|0> + b.|1>), 2.5e-1],
[|1>(x)|0>(x)(a.|0> + b.|1>), 2.5e-1],
[|0>(x)|1>(x)(a.|0> + b.|1>), 2.5e-1],
[|1>(x)|1>(x)(a.|0> + b.|1>), 2.5e-1]
```

Contents

Experiments

- A MacBook Pro machine with an Apple M4 Max chip and 48 GB of RAM was used.
- For constructing entanglement with 100 qubits, |AS4QC> is comparable with graph-based quantum simulators such as QuIDDPro and MQT Core DD, while array-based quantum simulators such as LIQ$Ui|\rangle$, QX, and ProjectQ could not do so.

Program	**Qubits**	**Unitary**	**Measurement**	**Time**
Entanglement	100	100	0	53ms
Quantum Teleportation	3	8	2	≈ 0
Entanglement Swapping	4	8	2	≈ 0
Quantum Secret Sharing	4	9	3	≈ 0
Quantum Relay Scheme	5	12	4	1ms
Bidirectional Teleportation	6	12	4	1ms
Quantum Network Coding	14	37	10	268ms
Grover's Search	5 10 15	133 1,430 11,973	0 0 0	10ms 1.2s 3.9m

Contents

Conclusion and Future Work

Conclusion

- |AS4QC> - an algebraic specification for quantum computation in Maude for modelling, symbolic and exact reasoning about, and verifying quantum systems.
- The ring $\mathbb{D}[\omega]$ to represent complex numbers, Dirac notation to represent quantum states and operators, and a set of rules to automate reasoning in Maude.
- Case studies to demonstrate the effectiveness and practicality of |AS4QC>.

Future Work

- Although a complex number can be algebraically represented by a quadruple (a, b, c, d) and a normalization factor k, many different choices of (a, b, c, d) and k may represent the same complex number.
- To model check quantum systems with |AS4QC> effectively, developing a unique representation for this algebraic form is required.

Thank You!