Reasoning about Quantum Protocols in QPEL

Robin Adams `robin@cs.ru.nl`

Radboud University

A type theory for denoting quantum programs, and effects on quantum systems.
First presented in [1]

Syntax

Types

A type represents a state space for a quantum computer.

$\boldsymbol{I}$	Unit type
$\boldsymbol{A} \otimes \boldsymbol{B}$	Pair of $\boldsymbol{A}$ and $\boldsymbol{B}$ (possibly entangled)
$\boldsymbol{A} + \boldsymbol{B}$	Either $\boldsymbol{A}$ or $\boldsymbol{B}$ (classical 'or')
qbit	Qubits

Terms

A term represents a quantum computation.

$\boldsymbol{x}$	Variable
$\boldsymbol{M} \otimes \boldsymbol{N}$	Separated state
$\mathbf{let}\ \boldsymbol{x} \otimes \boldsymbol{y} = \boldsymbol{M}\ \mathbf{in}\ \boldsymbol{N}$	Eliminator for $\boldsymbol{A} \otimes \boldsymbol{B}$
$\mathbf{inl}\,(\boldsymbol{M})$	Injection $\boldsymbol{A} \to \boldsymbol{A} + \boldsymbol{B}$
$\mathbf{inr}\,(\boldsymbol{M})$	Injection $\boldsymbol{B} \to \boldsymbol{A} + \boldsymbol{B}$
$\mathbf{case}\ \boldsymbol{M}\ \mathbf{of}\ \mathbf{inl}\,(\boldsymbol{x}) \mapsto \boldsymbol{N} \mid \mathbf{inr}\,(\boldsymbol{y}) \mapsto \boldsymbol{P}$	Eliminator for $\boldsymbol{A} + \boldsymbol{B}$
$\mathbf{measure}\ \boldsymbol{\phi}_1 \mapsto \boldsymbol{M}_1 \mid \cdots \mid \boldsymbol{\phi}_n \mapsto \boldsymbol{M}_n$	Make measurement then branch
$\mathbf{inlr}\,(\boldsymbol{M}, \boldsymbol{N})$	Returns the output of $\boldsymbol{M}$ or $\boldsymbol{N}$ (only if exactly one of $\boldsymbol{M}$, $\boldsymbol{N}$ terminates)
$\lvert\mathbf{0}\rangle$	New qubit
$\boldsymbol{U}\boldsymbol{M}$	Apply a quantum gate ($\boldsymbol{U}$ a $\mathbf{2}^{\boldsymbol{n}} \times \mathbf{2}^{\boldsymbol{n}}$ complex unitary matrix)

Effects

An effect represents a measurement that can be performed.

$\mathbf{0}$	Always false effect
$\boldsymbol{\phi} \oplus \boldsymbol{\psi}$	Sum of $\boldsymbol{\phi}$ and $\boldsymbol{\psi}$ (only if $\boldsymbol{\phi} \perp \boldsymbol{\psi}$)
$\boldsymbol{\phi}^{\perp}$	Orthocomplement of $\boldsymbol{\phi}$
$\boldsymbol{\phi} \otimes \boldsymbol{\psi}$	Tensor product
$\mathbf{case}\ \boldsymbol{M}\ \mathbf{of}\ \mathbf{inl}\,(\boldsymbol{x}) \mapsto \boldsymbol{\phi} \mid \mathbf{inr}\,(\boldsymbol{y}) \mapsto \boldsymbol{\psi}$	Perform one of two measurements depending on $\boldsymbol{M}$
$\lvert\mathbf{0}\rangle\,\boldsymbol{M}$	Measure qubit in standard basis

We write $\mathbf{1}$ for $\mathbf{0}^{\perp}$.

Judgements

QPEL has four judgement forms:

$\boldsymbol{\Gamma} \vdash \boldsymbol{M} : \boldsymbol{A}$	$\boldsymbol{M}$ is an algorithm taking inputs $\boldsymbol{\Gamma}$, giving output $\boldsymbol{A}$
$\boldsymbol{\Gamma} \vdash \boldsymbol{M} = \boldsymbol{N} : \boldsymbol{A}$	$\boldsymbol{M}$ and $\boldsymbol{N}$ give the same output to the same input
$\boldsymbol{\Gamma} \vdash \boldsymbol{\phi}\ \mathbf{pred}$	$\boldsymbol{\phi}$ is an effect that may be measured on $\boldsymbol{\Gamma}$
$\boldsymbol{\Gamma} \vdash \boldsymbol{\phi} \leqslant \boldsymbol{\psi}$	Probability of $\boldsymbol{\phi}$ is $\leqslant$ probability of $\boldsymbol{\psi}$ on all states of $\boldsymbol{\Gamma}$

We write $\boldsymbol{\Gamma} \vdash \boldsymbol{\phi} \Leftrightarrow \boldsymbol{\psi}$ for the two judgements $\boldsymbol{\Gamma} \vdash \boldsymbol{\phi} \leqslant \boldsymbol{\psi}$ and $\boldsymbol{\Gamma} \vdash \boldsymbol{\psi} \leqslant \boldsymbol{\phi}$.

The effects (measurements) are the *predicates* of our logic.
$\boldsymbol{\Gamma} \vdash \boldsymbol{\phi} \leqslant \boldsymbol{\psi}$ is the entailment relation.

Semantics

If we omit the type **qbit**, the models of QPEL are *state-and-effect triangles*

$$\begin{array}{ccc} \mathbf{EMod}_{\boldsymbol{E}}^{\mathrm{op}} & \rightleftarrows & \mathbf{Conv}_{\boldsymbol{E}} \\ & \boldsymbol{P} \searrow \quad \swarrow \boldsymbol{S} & \\ & \boldsymbol{\mathcal{V}} & \end{array}$$

With **qbit**, the rules are sound and complete for $\boldsymbol{\mathcal{V}} = \mathbf{CStar}_{\mathbf{CPU}}^{\mathrm{op}}$.

Structural Rules

QPEL is an *affine* type system. It satisfies Weakening and Exchange but *not* Contraction.

$$\text{(Weakening)}\ \frac{\boldsymbol{\Gamma} \vdash \boldsymbol{\mathcal{J}}}{\boldsymbol{\Delta} \vdash \boldsymbol{\mathcal{J}}}\ (\boldsymbol{\Gamma} \subseteq \boldsymbol{\Delta}) \qquad \text{(exchange)}\ \frac{\boldsymbol{\Gamma}, \boldsymbol{x} : \boldsymbol{A}, \boldsymbol{y} : \boldsymbol{B}, \boldsymbol{\Delta} \vdash \boldsymbol{\mathcal{J}}}{\boldsymbol{\Gamma}, \boldsymbol{y} : \boldsymbol{B}, \boldsymbol{x} : \boldsymbol{A}, \boldsymbol{\Delta} \vdash \boldsymbol{\mathcal{J}}}$$

$$\text{(Contraction)}\ \frac{\boldsymbol{\Gamma}, \boldsymbol{x} : \boldsymbol{A}, \boldsymbol{y} : \boldsymbol{A}, \boldsymbol{\Delta} \vdash \boldsymbol{\mathcal{J}}}{\boldsymbol{\Gamma}, \boldsymbol{z} : \boldsymbol{A}, \boldsymbol{\Delta} \vdash [\boldsymbol{z}/\boldsymbol{x}, \boldsymbol{z}/\boldsymbol{y}]\boldsymbol{\mathcal{J}}}$$

Data may be destroyed (by measurement).
Quantum data may *not* be duplicated (*No-cloning theorem*).

Computation Rules (based on [2])

We have the obvious $\boldsymbol{\beta}$- and $\boldsymbol{\eta}$-rules for $+$ and $\otimes$, plus:

$$\begin{aligned}
(\mathrm{id} + !)\mathbf{inlr}\,(\boldsymbol{M}, \boldsymbol{N}) &= \boldsymbol{M} \\
(! + \mathrm{id})\mathbf{inlr}\,(\boldsymbol{M}, \boldsymbol{N}) &= \boldsymbol{N} \\
\mathbf{inlr}\,((\mathrm{id} + !)\boldsymbol{M}, (! + \mathrm{id})\boldsymbol{M}) &= \boldsymbol{M} \\
(\mathbf{measure}\ {}^{n}_{i=1}\boldsymbol{\phi}_i \mapsto \boldsymbol{M}_i) &= (\mathbf{measure}\ {}^{n}_{i=1}\boldsymbol{\phi}_{p(i)} \mapsto \boldsymbol{M}_{p(i)}) \\
(\mathbf{measure}\ \boldsymbol{\phi}_1 \mapsto \boldsymbol{M}_1 \mid \cdots \mid \boldsymbol{\phi}_n \mapsto \boldsymbol{M}_n \mid \mathbf{0} \mapsto \boldsymbol{M}_{n+1}) & \\
\qquad = \mathbf{measure}\ \boldsymbol{\phi}_1 \mapsto \boldsymbol{M}_1 \mid \cdots \mid \boldsymbol{\phi}_n \mapsto \boldsymbol{M}_n & \\
(\mathbf{measure}\ \mathbf{1} \mapsto \boldsymbol{M}) &= \boldsymbol{M} \\
(\mathbf{measure}\ \boldsymbol{\phi} \oplus \boldsymbol{\psi} \mapsto \boldsymbol{M} \mid \cdots) &= (\mathbf{measure}\ \boldsymbol{\phi} \mapsto \boldsymbol{M} \mid \boldsymbol{\psi} \mapsto \boldsymbol{M} \mid \cdots) \\
\text{where } \boldsymbol{\phi} \text{ and } \boldsymbol{\psi} \text{ are scalars} &
\end{aligned}$$

$$\begin{aligned}
\mathbf{let}\ \boldsymbol{x} \otimes \boldsymbol{y} = \boldsymbol{D}(\boldsymbol{U}, \boldsymbol{V})(\boldsymbol{M} \otimes \boldsymbol{N})\ \mathbf{in}\ \langle\mathbf{0}|\,\boldsymbol{x} \otimes \boldsymbol{\phi}[\boldsymbol{y}] &\Leftrightarrow \langle\mathbf{0}|\,\boldsymbol{M} \otimes \boldsymbol{\phi}[\boldsymbol{U}\boldsymbol{N}] \\
\langle\mathbf{0}|\,\boldsymbol{X}\boldsymbol{M} &\Leftrightarrow \langle\mathbf{1}|\,\boldsymbol{M} \\
(\mathbf{let}\ \boldsymbol{x} \otimes \boldsymbol{y} = \boldsymbol{D}(\boldsymbol{U}, \boldsymbol{V})(\boldsymbol{M} \otimes \boldsymbol{N})\ \mathbf{in}\ \boldsymbol{y}) &= \begin{pmatrix} \mathbf{measure} & \langle\mathbf{0}|\,\boldsymbol{M} \mapsto \boldsymbol{U}\boldsymbol{N} \\ & \mid \langle\mathbf{1}|\,\boldsymbol{M} \mapsto \boldsymbol{V}\boldsymbol{N} \end{pmatrix} \\
\langle\mathbf{0} \mid \mathbf{0}\rangle &\Leftrightarrow \mathbf{1} \\
\boldsymbol{D}(\boldsymbol{U}, \boldsymbol{V})(\lvert\mathbf{0}\rangle \otimes \boldsymbol{N}) &= \lvert\mathbf{0}\rangle \otimes \boldsymbol{U}\boldsymbol{N} \\
\mathbf{swap}\,(\boldsymbol{M} \otimes \boldsymbol{N}) &= \boldsymbol{N} \otimes \boldsymbol{M} \\
\boldsymbol{I}\boldsymbol{M} &= \boldsymbol{M} \\
\boldsymbol{U}(\boldsymbol{V}\boldsymbol{M}) &= (\boldsymbol{U}\boldsymbol{V})\boldsymbol{M} \\
(\boldsymbol{U} \otimes \boldsymbol{V})(\boldsymbol{M} \otimes \boldsymbol{N}) &= \boldsymbol{U}\boldsymbol{M} \otimes \boldsymbol{V}\boldsymbol{N}
\end{aligned}$$

where $\boldsymbol{D}(\boldsymbol{U}, \boldsymbol{V}) = \begin{pmatrix} \boldsymbol{U} & \boldsymbol{O} \\ \boldsymbol{O} & \boldsymbol{V} \end{pmatrix}$.

Example — The Bell State

$$\mathbf{CNOT} \stackrel{\mathrm{def}}{=} \boldsymbol{D}(\boldsymbol{I}, \boldsymbol{X}) \qquad \mathbf{Bell} \stackrel{\mathrm{def}}{=} \mathbf{CNOT}(\boldsymbol{H}\,\lvert\mathbf{0}\rangle \otimes \lvert\mathbf{0}\rangle)$$

We can express the fact that the qubits in a Bell state are 7 entangled as follows:

$$\begin{aligned}
&(\mathbf{let}\ \boldsymbol{x} \otimes \boldsymbol{y} = \mathbf{Bell}\ \mathbf{in}\ \langle\mathbf{0}|\,\boldsymbol{x}) \\
\Leftrightarrow &(\mathbf{let}\ \boldsymbol{x} \otimes \boldsymbol{y} = \mathbf{CNOT}(\boldsymbol{H}\,\lvert\mathbf{0}\rangle \otimes \lvert\mathbf{0}\rangle)\ \mathbf{in}\ \langle\mathbf{0}|\,\boldsymbol{x} \otimes \langle\mathbf{0}|\,\boldsymbol{y}) \\
\Leftrightarrow &\langle\mathbf{0}|\,\boldsymbol{H}\,\lvert\mathbf{0}\rangle \otimes \langle\mathbf{0} \mid \mathbf{0}\rangle \\
\Leftrightarrow &\langle\mathbf{0}|\,\boldsymbol{H}\,\lvert\mathbf{0}\rangle \otimes \mathbf{1} \\
\Leftrightarrow &\mathbf{let}\ \boldsymbol{x} \otimes \boldsymbol{y} = \mathbf{CNOT}(\boldsymbol{H}\,\lvert\mathbf{0}\rangle \otimes \lvert\mathbf{0}\rangle)\ \mathbf{in}\ \langle\mathbf{0}|\,\boldsymbol{x} \otimes \mathbf{1} \\
\Leftrightarrow &\mathbf{let}\ \boldsymbol{x} \otimes \boldsymbol{y} = \mathbf{Bell}\ \mathbf{in}\ \langle\mathbf{0}|\,\boldsymbol{x}
\end{aligned}$$

Quantum Teleportation

The **inlr** construction allows us to reason case-by-case:

$$\boldsymbol{F}_1(\boldsymbol{x}) \stackrel{\mathrm{def}}{=} \mathbf{let}\ \boldsymbol{x} \otimes \boldsymbol{y} \otimes \boldsymbol{z} = \mathbf{prepare}\,(\boldsymbol{x})\ \mathbf{in}\ \mathbf{measure} \begin{cases} \langle\mathbf{00}|\,\boldsymbol{x}\boldsymbol{y} \mapsto \mathbf{inl}\,(\boldsymbol{z}) \\ (\langle\mathbf{00}|\,\boldsymbol{x}\boldsymbol{y})^{\perp} \mapsto \mathbf{inr}\,(\langle\rangle) \end{cases} = \mathbf{measure} \begin{cases} 1/4 \mapsto \mathbf{inl}\,(\boldsymbol{x}) \\ 3/4 \mapsto \mathbf{inr}\,(\langle\rangle) \end{cases}$$

$$\boldsymbol{F}_2(\boldsymbol{x}) \stackrel{\mathrm{def}}{=} \mathbf{let}\ \boldsymbol{x} \otimes \boldsymbol{y} \otimes \boldsymbol{z} = \mathbf{prepare}\,(\boldsymbol{x})\ \mathbf{in}\ \mathbf{measure} \begin{cases} \langle\mathbf{00}|\,\boldsymbol{x}\boldsymbol{y} \mapsto \mathbf{inl}\,(\langle\rangle) \\ \langle\mathbf{01}|\,\boldsymbol{x}\boldsymbol{y} \mapsto \mathbf{inr}\,(\mathbf{inl}\,(\boldsymbol{X}\boldsymbol{z})) \\ \langle\mathbf{1}|\,\boldsymbol{x} \mapsto \mathbf{inr}\,(\mathbf{inr}\,(\langle\rangle)) \end{cases} = \mathbf{measure} \begin{cases} 1/4 \mapsto \mathbf{inl}\,(\langle\rangle) \\ 1/4 \mapsto \mathbf{inr}\,(\mathbf{inl}\,(\boldsymbol{x})) \\ 1/2 \mapsto \mathbf{inr}\,(\mathbf{inr}\,(\langle\rangle)) \end{cases}$$

$$\mathbf{THEREFORE}$$

$$(\boldsymbol{\nabla} + \mathrm{id})(\mathbf{inlr}\,(\boldsymbol{F}_1(\boldsymbol{x}), \boldsymbol{F}_2(\boldsymbol{x})))$$

$$= \mathbf{let}\ \boldsymbol{x} \otimes \boldsymbol{y} \otimes \boldsymbol{z} = \mathbf{prepare}\,(\boldsymbol{x})\ \mathbf{in}\ \mathbf{measure} \begin{cases} \langle\mathbf{00}|\,\boldsymbol{x}\boldsymbol{y} \mapsto \mathbf{inl}\,(\boldsymbol{z}) \\ \langle\mathbf{01}|\,\boldsymbol{x}\boldsymbol{y} \mapsto \mathbf{inl}\,(\boldsymbol{X}\boldsymbol{z}) \\ \langle\mathbf{1}|\,\boldsymbol{x} \mapsto \mathbf{inr}\,(\langle\rangle) \end{cases} = \mathbf{measure} \begin{cases} 1/2 \mapsto \mathbf{inl}\,(\boldsymbol{x}) \\ 1/2 \mapsto \mathbf{inr}\,(\langle\rangle) \end{cases}$$

Handling the other two cases similarly, we build up to

$$\boldsymbol{x} : \mathbf{qbit} \vdash \mathbf{teleport}\,(\boldsymbol{x}) = \boldsymbol{x} : \mathbf{qbit}$$

$$\begin{aligned}
\mathbf{prepare}\,(\boldsymbol{x}) &\stackrel{\mathrm{def}}{=} \mathbf{let}\ \boldsymbol{y} \otimes \boldsymbol{z} = \mathbf{Bell}\ \mathbf{in} \\
&\quad \mathbf{let}\ \boldsymbol{x} \otimes \boldsymbol{y} = \mathbf{CNOT}(\boldsymbol{x} \otimes \boldsymbol{y})\ \mathbf{in} \\
&\quad \mathbf{let}\ \boldsymbol{x} = \boldsymbol{H}\boldsymbol{x}\ \mathbf{in} \\
&\quad \boldsymbol{x} \otimes \boldsymbol{y} \otimes \boldsymbol{z} \\
\mathbf{teleport}\,(\boldsymbol{x}) &\stackrel{\mathrm{def}}{=} \\
&\quad \mathbf{let}\ \boldsymbol{x} \otimes \boldsymbol{y} \otimes \boldsymbol{z} = \mathbf{prepare}\,(\boldsymbol{x})\ \mathbf{in} \\
&\quad \mathbf{measure} \\
&\quad \langle\mathbf{0}|\,\boldsymbol{x} \otimes \langle\mathbf{0}|\,\boldsymbol{y} \mapsto \boldsymbol{z} \\
&\quad \langle\mathbf{0}|\,\boldsymbol{x} \otimes \langle\mathbf{1}|\,\boldsymbol{y} \mapsto \boldsymbol{X}\boldsymbol{z} \\
&\quad \langle\mathbf{1}|\,\boldsymbol{x} \otimes \langle\mathbf{0}|\,\boldsymbol{y} \mapsto \boldsymbol{Z}\boldsymbol{z} \\
&\quad \langle\mathbf{1}|\,\boldsymbol{x} \otimes \langle\mathbf{1}|\,\boldsymbol{y} \mapsto \boldsymbol{Z}(\boldsymbol{X}\boldsymbol{z})
\end{aligned}$$

Bibliography

- Robin Adams. Qpel: Quantum programming and effect language. In *11th Workshop on Quantum Physics and Logic*, pages 133–153, 2014.
- Sam Staton. Algebraic effects, linearity, and quantum programming languages. In *POPL'15*, pages 395–406, 2015.