Quantum Alternation: Prospects and Problems

Costin Bădescu
(Joint work with Prakash Panangaden)

McGill University

July 15, 2015

Quantum Control

- Two aspects of any computational mechanism:

  data manipulation + control flow.

- In a quantum programming language, classical control flow can be defined using measurements:

  $$\textbf{measure } q \textbf{ then } P \textbf{ else } Q$$

- Does there exist a notion of alternation which operates in the absence of measurement?

  $$\textbf{if } q \textbf{ then } P \textbf{ else } Q$$

  The state of q determines how P and Q are applied.

Quantum Control

- Alternative paradigm: **quantum control** or **quantum alternation**.
- Differs from usual "quantum data, classical control" paradigm.
- The initial formulation of the concept is vague.
- No clear formal definition of quantum alternation.
- Concept may be useful in understanding the structure of quantum programs.

Axiomatisation

- Peter Selinger's QPL as base programming language.
- P and Q expressions in QPL, $q : \mathbf{qbit}$ a qubit.
- **Condition 1**: Quantum alternation has the following typing judgement, where Ψ is a procedure context and Γ and Γ' are typing contexts:

$$\frac{\Psi \vdash \langle \Gamma \rangle\, P\, \langle \Gamma' \rangle \qquad \Psi \vdash \langle \Gamma \rangle\, Q\, \langle \Gamma' \rangle}{\Psi \vdash \langle q : \mathbf{qbit}, \Gamma \rangle\ \mathbf{if}\ q\ \mathbf{then}\ P\ \mathbf{else}\ Q\, \langle q : \mathbf{qbit}, \Gamma' \rangle}$$

- P and Q cannot access q.

Axiomatisation

- Alternation denoted by

$$\mathrm{Alt}_q(T_0, T_1) : B(\mathbf{qbit} \otimes \mathcal{H}) \to B(\mathbf{qbit} \otimes \mathcal{K})$$

  where $T_0, T_1 : B(\mathcal{H}) \to B(\mathcal{K})$ are quantum operations and $q : \mathbf{qbit}$ is a qubit.

- The state of q should affect the outcome of the alternation of P and Q.

- **Condition 2**: If the qubit q is in a classical state Π_i with $i \in \{0, 1\}$, then $\mathrm{Alt}_q(T_0, T_1) = \mathrm{id} \otimes T_i$; the alternation reduces to operation T_i on $B(\mathcal{H})$.

Axiomatisation

- Conditions 1 & 2 not sufficient:

$$\mathrm{Alt}_q(T_0, T_1) :: \rho = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \begin{bmatrix} T_0(a) & \star \\ \star & T_1(d) \end{bmatrix}.$$

- A quantum operation T is reversible if $T(\rho) = U\rho U^\dagger$ with U unitary.
- **Condition 3**: If T_0 and T_1 are reversible, then $\mathrm{Alt}_q(T_0, T_1)$ is reversible.

Closed Systems

- Let $U_0, U_1 \in B(\mathcal{H})$ be unitary operators on a Hilbert space $\mathcal{H}$. Given a qubit $q : \mathbf{qbit}$, define the alternation $\mathrm{Alt}_q(U_0, U_1)$ by

$$\mathrm{Alt}_q(U_0, U_1) = \Pi_0 \otimes U_0 + \Pi_1 \otimes U_1.$$

  Π_i is the projection onto the subspace generated by $|i\rangle$.

- Alternates U_0 and U_1 according to q:

$$\mathrm{Alt}_q(U_0, U_1) :: |0\rangle \otimes x + |1\rangle \otimes y \;\mapsto\; |0\rangle \otimes U_0\, x + |1\rangle \otimes U_1\, y$$

- Denoted by

$$\textbf{if } q_0 \textbf{ then } q_1 \mathrel{*}= U_0 \textbf{ else } q_1 \mathrel{*}= U_1$$

Closed Systems

- Let $\mathbf{qbit}^n = \mathbf{qbit} \otimes \ldots \otimes \mathbf{qbit}$, $\ell = 2^n - 1$.
- $\Pi_0, \ldots, \Pi_\ell$ the classical states of $\mathbf{qbit}^n$.
- Given $\bar{q} : \mathbf{qbit}^n$, the alternation of unitary operators $U_0, \ldots, U_\ell \in B(\mathcal{H})$ with respect to $\bar{q}$ is defined by

$$\mathsf{Alt}_{\bar{q}}(U_0, \ldots, U_\ell) = \sum_{k=0}^{\ell} \Pi_k \otimes U_k.$$

- Corresponds to a **case** statement:

$$\textbf{case } \bar{q} \textbf{ of } |k\rangle \to P_k$$

Examples

- If U is a unitary operator and $q_0, q_1 : \textbf{qbit}$ are two qubits, then

$$\textbf{if } q_0 \textbf{ then skip else } q_1 \mathrel{*}= U$$

  defines a controlled-U operation.

- Thus, if N is the NOT gate, two nested **if** statements can be used to define the Toffoli gate:

$$\textbf{if } q_0 \textbf{ then skip else if } q_1 \textbf{ then skip else } q_2 \mathrel{*}= N$$

- Quantum alternation generalizes controlled unitary operations.

Examples

- Let $f : \{0,1\}^n \to \{0,1\}$ be a boolean function.
- For each $x \in \{0,1\}^n$, $U_x : \textbf{qbit} \to \textbf{qbit}$ transposes $|0\rangle$ & $|f(x)\rangle$.
- Thus, $\textbf{case } \bar{q}_0 \textbf{ of } |x\rangle \to q_1 \mathrel{*}= U_x$ defines the unitary

$$U_f = |x, y\rangle \mapsto |x, y \oplus f(x)\rangle.$$

- The Deutsch–Jozsa algorithm:

$$\begin{aligned}
&\textbf{new qbit}^n\ \bar{q}_0\\
&\textbf{new qbit}\ q_1\\
&\bar{q}_0 \mathrel{*}= H^{\otimes n}\\
&q_1 \mathrel{*}= H \circ N\\
&\textbf{case } \bar{q}_0 \textbf{ of } |x\rangle \to q_1 \mathrel{*}= U_x\\
&\bar{q}_0 \mathrel{*}= H^{\otimes n}
\end{aligned}$$

Examples

- The conditional statement

$$\textbf{if } q_0 \textbf{ then skip else } q_1 \mathrel{*}= e^{i\theta}$$

  defines a controlled phase.
- **skip** and $q_1 \mathrel{*}= e^{i\theta}$ are physically indistinguishable as quantum operations.
- Quantum alternation is not physical.

Semantics

- **Problem**: Can this form of alternation be extended to open quantum systems?
- Given quantum operations $T_0, T_1 : B(\mathcal{H}) \to B(\mathcal{K})$ and a qubit $q : \mathbf{qbit}$, construct a quantum operation:

$$\mathrm{Alt}_q(T_0, T_1) : B(\mathbf{qbit} \otimes \mathcal{H}) \to B(\mathbf{qbit} \otimes \mathcal{K}).$$

- Initial idea (due to Nengkun Yu): Define a quantum programming language with quantum alternation and recursion.
- In this case: Extend QPL with quantum alternation.

Semantics

Different representations of CP maps:

- (Kraus) $T(\rho) = \sum_k E_k \rho E_k^\dagger$.
- (Stinespring) $T(\rho) = V^\dagger(\rho \otimes \mathbf{1}_\mathcal{E})V$.
- (Idem) $T(\rho) = \mathrm{Tr}_\mathcal{E}\, U(\rho \otimes |\xi\rangle\langle\xi|)U^\dagger$.
- (Arveson) If $T(\rho) = V^\dagger(\rho \otimes \mathbf{1}_\mathcal{E})V$, then

$$S \leqslant T \iff \exists\, \mathrm{D}_T(S) \text{ s.t. } S(\rho) = V^\dagger(\rho \otimes \mathbf{1}_\mathcal{E})\,\mathrm{D}_T(S)V.$$

Semantics of Quantum Alternation

- A finite set $\mathcal{T}$ of nonzero bounded operators from $\mathcal{H}$ to $\mathcal{K}$ defines a superoperator $T : B(\mathcal{H}) \to B(\mathcal{K})$ by

$$T(\rho) = \sum_{E \in \mathcal{T}} E \rho E^{\dagger} \qquad \text{if} \qquad \sum_{E \in \mathcal{T}} E^{\dagger} E \leqslant \mathbf{1}\,. \tag{1}$$

  We say $\mathcal{T}$ is a *decomposition of* T.

- By convention, $\varnothing$ corresponds to the 0 CP map.

- Define a category $\mathbf{C}$:
  - $\mathrm{Ob}(\mathbf{C})$ = finite-dimensional Hilbert spaces $\mathcal{H}, \mathcal{K}$,
  - $\mathrm{Ar}(\mathbf{C})$ = decompositions $\mathcal{T}$ of superoperators $T : B(\mathcal{H}) \to B(\mathcal{K})$.

Semantics of Quantum Alternation

- Define the **quantum alternation** of two Kraus decompositions $\mathcal{S}, \mathcal{T} : \mathcal{H} \to \mathcal{K}$ to be the morphism $\mathcal{S} \bullet \mathcal{T} : \textbf{qbit} \otimes \mathcal{H} \to \textbf{qbit} \otimes \mathcal{K}$ defined by

$$\mathcal{S} \bullet \mathcal{T} = \left\{ \Pi_0 \otimes \frac{E}{\sqrt{|\mathcal{T}|}} + \Pi_1 \otimes \frac{F}{\sqrt{|\mathcal{S}|}} : E \in \mathcal{S}, F \in \mathcal{T} \right\}.$$

  The projections Π_0 and Π_1 are determined by the qubit $q : \textbf{qbit}$ used in the alternation.

Semantics of QPL

Semantics of QPL with quantum alternation:

$$
\begin{aligned}
&[\![P; Q]\!] &&: \sigma \to \tau &&= [\![Q]\!] \circ [\![P]\!] \\
&[\![\textbf{skip}]\!] &&: \sigma \to \sigma &&= \{\mathrm{id}\} \\
&[\![\textbf{new bit } b := 0]\!] &&: \sigma \to \sigma \oplus \sigma &&= \{\mathrm{in}_0\} \\
&[\![\textbf{new qbit } q := 0]\!] &&: \sigma \to \textbf{qbit} \otimes \sigma &&= \{|0\rangle \otimes -\} \\
&[\![\textbf{discard } q]\!] &&: \textbf{qbit} \otimes \sigma \to \sigma &&= \{\langle 0| \otimes \mathrm{id},\ \langle 1| \otimes \mathrm{id}\} \\
&[\![\textbf{merge}]\!] &&: \sigma \oplus \sigma \to \sigma &&= \{\mathrm{in}_0^\dagger, \mathrm{in}_1^\dagger\} \\
&[\![\textbf{measure } q]\!] &&: \sigma \to \sigma \oplus \sigma &&= \{\mathrm{in}_0 \circ \Pi_0,\ \mathrm{in}_1 \circ \Pi_1\} \\
&[\![q \mathrel{*}= U]\!] &&: \sigma \to \sigma &&= \{U\} \\
&[\![\textbf{if } q \textbf{ then } P \textbf{ else } Q]\!] &&: \textbf{qbit} \otimes \sigma \to \textbf{qbit} \otimes \tau &&= [\![P]\!] \bullet [\![Q]\!]
\end{aligned}
$$

Semantics of Superoperators

- Can quantum alternation be defined as a function on pairs of superoperators?
- $\mathcal{T} \simeq \mathcal{S}$ iff the corresponding superoperators are equal.
- $\{U_0\} \bullet \{V_0\} \simeq \{U_1\} \bullet \{V_1\}$ may not hold even if $\{U_0\} \simeq \{U_1\}$ and $\{V_0\} \simeq \{V_1\}$.
- Quantum alternation is not stable under the extensional equality of decompositions.
- There is no structural superoperator semantics which satisfies the definition of alternation given for closed systems.

Recursion

- Recursion in QPL is based on the Löwner order on superoperators. Is quantum alternation compatible with recursion?
- **No.** The quantum alternation operation is not monotone with respect to the Löwner order on CP maps.
- Given decompositions $\mathcal{S} = \{U\}$ and $\mathcal{T} = \{V\}$, let ρ be a state on $\mathbf{qbit} \otimes \mathcal{H}$ defined by
$$\rho = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$
where $b \neq 0$. Then $\mathcal{S} \leqslant \mathcal{S}$ and $\varnothing \leqslant \mathcal{T}$, but
$$(\mathcal{S} \bullet \mathcal{T} - \mathcal{S} \bullet \varnothing)(\rho) = \begin{bmatrix} 0 & UbV^\dagger \\ VcU^\dagger & VdV^\dagger \end{bmatrix}.$$
Since $UbV^\dagger \neq 0$, $(\mathcal{S} \bullet \mathcal{T} - \mathcal{S} \bullet \varnothing)(\rho)$ is not positive.

Related Work

- QML defined by T. Altenkirch and J. Grattage.
  - Semantics based on category **FQC**.
  - Representation of superoperators: $T(\rho) = \mathrm{Tr}_{\mathcal{E}}\, U(\rho \otimes |\xi\rangle\langle\xi|)U^{\dagger}$.
  - Only *strict morphisms* ($\dim \mathcal{E} = 1$) can be alternated.
  - Depends on an *orthogonality judgment*.

- QGCL defined by M. Ying, N. Yu, and Y. Feng.
  - Semantics based on *operator-valued functions*:
    $$[n] \to B(\mathcal{H}) \text{ s.t. } k \mapsto E_k.$$
  - Definition of alternation generalized to n branches.
  - Extract a superoperator semantics by forgetting the decompositions – alternation is not a *function* on pairs of superoperators.
  - Use a coin system; alternation becomes a binding operation.

Conclusion

What is the verdict on quantum alternation in open systems?

- Not directly definable on pairs of superoperators.
- Not physically grounded.
- Not compatible with recursion.
- Not evidently useful for designing quantum algorithms.