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:
  
  \[
  \text{measure } q \text{ then } P \text{ else } Q
  \]
- Does there exist a notion of alternation which operates in the absence of measurement?
  
  \[
  \text{if } q \text{ then } P \text{ else } Q
  \]

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, \( q : \text{qbit} \) a qubit.
- **Condition 1:** Quantum alternation has the following typing judgement, where \( \Psi \) is a procedure context and \( \Gamma \) and \( \Gamma' \) are typing contexts:

\[
\Psi \vdash \langle \Gamma \rangle P \langle \Gamma' \rangle \quad \Psi \vdash \langle \Gamma \rangle Q \langle \Gamma' \rangle \\
\Psi \vdash \langle q : \text{qbit}, \Gamma \rangle \text{ if } q \text{ then } P \text{ else } Q \langle q : \text{qbit}, \Gamma' \rangle
\]

- \( P \) and \( Q \) cannot access \( q \).
Axiomatisation

- Alternation denoted by

\[ \text{Alt}_q(T_0, T_1) : B(\text{qbit} \otimes \mathcal{H}) \rightarrow B(\text{qbit} \otimes \mathcal{K}) \]

where \( T_0, T_1 : B(\mathcal{H}) \rightarrow B(\mathcal{K}) \) are quantum operations and \( q : \text{qbit} \) 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 \( \Pi_i \) with \( i \in \{0, 1\} \), then \( \text{Alt}_q(T_0, T_1) = \text{id} \otimes T_i \); the alternation reduces to operation \( T_i \) on \( B(\mathcal{H}) \).
Axiomatisation

- Conditions 1 & 2 not sufficient:

\[
\text{Alt}_q(T_0, T_1) \:: \rho = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto \begin{bmatrix} T_0(a) & * \\ * & T_1(d) \end{bmatrix}.
\]

- 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 \( \text{Alt}_q(T_0, T_1) \) 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 $q: \text{qbit}$, define the alternation $\text{Alt}_q(U_0, U_1)$ by

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

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

- Alternates $U_0$ and $U_1$ according to $q$:

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

- Denoted by

$$\text{if } q_0 \text{ then } q_1 *= U_0 \text{ else } q_1 *= U_1$$
Closed Systems

- Let \( \text{qbit}^n = \text{qbit} \otimes \ldots \otimes \text{qbit} \), \( \ell = 2^n - 1 \).

- \( \Pi_0, \ldots, \Pi_\ell \) the classical states of \( \text{qbit}^n \).

- Given \( \bar{q} : \text{qbit}^n \), the alternation of unitary operators \( U_0, \ldots, U_\ell \in B(\mathcal{H}) \) with respect to \( \bar{q} \) is defined by

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

- Corresponds to a \textbf{case} statement:

\[
\text{case } \bar{q} \text{ of } |k\rangle \rightarrow P_k
\]
Examples

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

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

defines a controlled-$U$ operation.

- Thus, if $N$ is the NOT gate, two nested \texttt{if} statements can be used to define the Toffoli gate:

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

- Quantum alternation generalizes controlled unitary operations.
Examples

- Let \( f : \{0, 1\}^n \rightarrow \{0, 1\} \) be a boolean function.

- For each \( x \in \{0, 1\}^n \), \( U_x : \text{qbit} \rightarrow \text{qbit} \) transposes \( |0\rangle \) & \( |f(x)\rangle \).

- Thus, case \( \bar{q}_0 \) of \( |x\rangle \rightarrow q_1 \ast= U_x \) defines the unitary

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

- The Deutsch–Jozsa algorithm:

```plaintext
new qbit^n \bar{q}_0
new qbit q_1
\bar{q}_0 \ast= H^{\otimes n}
q_1 \ast= H \circ N
case \bar{q}_0 \ of \ |x\rangle \rightarrow q_1 \ast= U_x
\bar{q}_0 \ast= H^{\otimes n}
```
Examples

- The conditional statement

  \[
  \text{if } q_0 \text{ then skip else } q_1 \ast = e^{i\theta}
  \]

  defines a controlled phase.

- \textbf{skip} and \( q_1 \ast = e^{i\theta} \) 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 $q : \text{qbit}$, construct a quantum operation:

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

- 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)** \( T(\rho) = V^\dagger (\rho \otimes 1_E) V. \)

- **(Idem)** \( T(\rho) = \text{Tr}_E U (\rho \otimes |\xi\rangle \langle \xi|) U^\dagger. \)

- **(Arveson)** If \( T(\rho) = V^\dagger (\rho \otimes 1_E) V, \) then

\[
S \preceq T \iff \exists D_T(S) \text{ s.t. } S(\rho) = V^\dagger (\rho \otimes 1_E) D_T(S) V.
\]
A finite set $\mathcal{T}$ of nonzero bounded operators from $\mathcal{H}$ to $\mathcal{K}$ defines a superoperator $T : B(\mathcal{H}) \rightarrow B(\mathcal{K})$ by

$$T(\rho) = \sum_{E \in \mathcal{T}} E \rho E^\dagger$$

if

$$\sum_{E \in \mathcal{T}} E^\dagger E \leq 1.$$

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

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

Define a category $\mathcal{C}$:
- $\text{Ob}(\mathcal{C}) = \text{finite-dimensional Hilbert spaces } \mathcal{H}, \mathcal{K}$,
- $\text{Ar}(\mathcal{C}) = \text{decompositions } \mathcal{T} \text{ of superoperators } T : B(\mathcal{H}) \rightarrow B(\mathcal{K})$. 
Define the **quantum alternation** of two Kraus decompositions $S, T : \mathcal{H} \rightarrow \mathcal{K}$ to be the morphism $S \cdot T : \text{qbit} \otimes \mathcal{H} \rightarrow \text{qbit} \otimes \mathcal{K}$ defined by

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

The projections $\Pi_0$ and $\Pi_1$ are determined by the qubit $q : \text{qbit}$ used in the alternation.
Semantics of QPL

Semantics of QPL with quantum alternation:

\[
[P; Q] : \sigma \rightarrow \tau = [Q] \circ [P] \\
\text{[skip]} : \sigma \rightarrow \sigma = \{\text{id}\} \\
[\text{new bit } b := 0] : \sigma \rightarrow \sigma \oplus \sigma = \{\text{in}_0\} \\
[\text{new qbit } q := 0] : \sigma \rightarrow \text{qbit} \otimes \sigma = \{|0\rangle \otimes -\} \\
[\text{discard } q] : \text{qbit} \otimes \sigma \rightarrow \sigma = \{\langle 0| \otimes \text{id}, \langle 1| \otimes \text{id}\} \\
[\text{merge}] : \sigma \oplus \sigma \rightarrow \sigma = \{\text{in}_0^\dagger, \text{in}_1^\dagger\} \\
[\text{measure } q] : \sigma \rightarrow \sigma \oplus \sigma = \{\text{in}_0 \circ \Pi_0, \text{in}_1 \circ \Pi_1\} \\
[q *= U] : \sigma \rightarrow \sigma = \{U\} \\
[\text{if } q \text{ then } P \text{ else } Q] : \text{qbit} \otimes \sigma \rightarrow \text{qbit} \otimes \tau = [P] \bullet [Q]
\]
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 $S = \{U\}$ and $T = \{V\}$, let $\rho$ be a state on qbit $\otimes \mathcal{H}$ defined by

$$\rho = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

where $b \neq 0$. Then $S \leq S$ and $\emptyset \leq T$, but

$$(S \bullet T - S \bullet \emptyset)(\rho) = \begin{bmatrix} 0 & UbV^\dagger \\ VcU^\dagger & VdV^\dagger \end{bmatrix}.$$  

Since $UbV^\dagger \neq 0$, $(S \bullet T - S \bullet \emptyset)(\rho)$ is not positive.
Related Work

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

- QGCL defined by M. Ying, N. Yu, and Y. Feng.
  - Semantics based on operator-valued functions:
    $$[n] \rightarrow B(\mathcal{H}) \text{ s.t. } k \mapsto E_k.$$  
  - 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.