On Quantum Non-locality: a formal approach

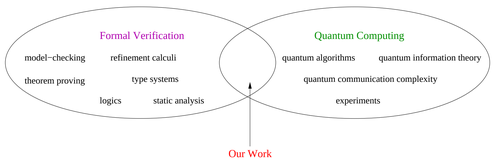
Anya Tafliovich, University of Toronto
http://www.cs.toronto.edu/~anya/
anya@cs.toronto.edu

Abstract

Quantum pseudo-telepathy is an intriguing phenomenon which results from the application of quantum information theory to communication complexity. To demonstrate this phenomenon researchers in the field of quantum communication complexity devised a number of quantum non-locality games. The setting of these games is as follows: the players are separated so that no communication between them is possible and are given a certain computational task. When the players have access to a quantum resource called entanglement, they can accomplish the task: something that is impossible in a classical setting. To an observer who is unfamiliar with the laws of quantum mechanics it seems that the players employ some sort of telepathy; that is, they somehow exchange information without sharing a communication channel.

This works provides a formal framework for specifying, implementing, and analyzing quantum non-locality games.

We look at quantum non-locality in the context of formal methods of program development, or programming methodology. This is the field of computer science concerned with applications of mathematics and logic to software engineering tasks. In particular, the formal methods provide tools to formally express specifications, prove correctness of implementations, and reason about various properties of specifications (e.g. implementability) and implementations (e.g. time and space complexity).



Formal Verification

Formal Verification is the field of computer science concerned with mathematics and modeling applicable to the specification, design, and verification of software and hardware. Why study it?

- develop provably correct software and hardware
- formally reason about properties of software and hardware systems
- aid in design and modeling of software and hardware systems
- save millions of dollars in software and hardware maintenance
- and more ...

Today formal methods are widely applied to systems of vaious scales: from small, safety-critical systems (heart monitors) to detailed specification, design, and verification of critical parts of very large systems (avionics and aerospace).

Quantum Computing

Quantum Computing is computing on any device that makes use of quantum mechanical phenomena. Why study it?

- faster algorithms
  - exponentially faster algorithms
  - quadratic speed-up for NP-complete algorithms
  - ...
- (pseudo-)telepathy
- secure cryptography
- exponential savings in communication complexity
- and more ...

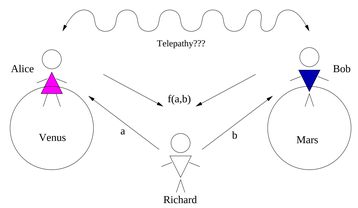
Theory of Quantum Programming

The goal our work is to develop a complete Quantum Predicative Programming theory, a unified formal framework which allows us to:

- write specifications
- develop algorithms/programs
- prove correctness
- prove time complexity
- prove space complexity
- prove communication complexity
- perform probabilistic analysis
- and more ...

for both classical and quantum systems. Quantum Predicative Programming is a recent generalization of the well-established predicative programming ([1, 2]).

Pseudo-Telepathy Games



- Alice and Bob play against the referee Richard
- task: given inputs x_a and x_b, compute $f(x_a, x_b)$
- Alice and Bob can talk *before* the experiment, but *no* communication is allowed *during* the experiment
- we can prove that (classically) it is highly unlikely that Alice and Bob win the game
- experiments show that they win every single time... telepathy?

We formalize the game as a distributed quantum program and calculate the odds of winning.

Background: Predicative Programming [1]

- start with a *specification*: what we want
- end with a *program*/algorithm/implementation: how we do it
- *refinement*: move step by step from specification to program, so that each step is justified by a law
- *result*: correct program
- for *free*: time, space, probabilistic, etc. analysis

Example:

Specification:	$P :== x \geq 0 \Rightarrow x' = 0$
Implementation:	$P \Leftarrow$ **if** $x = 0$ **then** *ok* **else** $x := x - 1;\ P$
Computational complexity:	$T :== x \geq 0 \wedge t' \leq t + x \vee x < 0 \wedge t' = \infty$
Proving complexity:	$T \Leftarrow$ **if** $x = 0$ **then** *ok* **else** $x := x - 1;\ t := t + 1;\ T$

Background: Probabilistic Predicative Programming [2]

Probabilistic Predicative Programming is a generalization of Predicative Programming to probabilistic computation. An interesting application: formal reasoning about veridical paradoxes.

Example: the Monty Hall Paradox

- step 0: There are three doors; behind two of them there is a goat, behind the third one – the prize
- step 1: Contestant chooses a door
- step 2: Monty opens one of the *other* two doors: the one with a goat
- step 3: Contestant can: stay with the previous choice or change her mind

- most people say: Does not matter!
- those who know the correct answer say: Switch!
- we say: Formalize and Calculate!

Don't switch:

$p := rand\ 3;$
$c := rand\ 3;$
if $c = p$ **then** $m := c \oplus 1 \vee m := c \oplus 2$
else $m := 3 - c - p;$
ok;
$c = p$
$:== 1/3$

Switch:

$p := rand\ 3;$
$c := rand\ 3;$
if $c = p$ **then** $m := c \oplus 1 \vee m := c \oplus 2$
else $m := 3 - c - p;$
$c := 3 - c - m;$
$c = p$
$:== 2/3$

Quantum Predicative Programming [3, 4, 5]

Add building blocks to programs (implemented specifications):

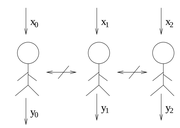
- $\psi := |0\rangle^{\otimes n}$ (initialization)
- $\psi := U\psi$ (unitary transformation)
- $\mathbf{measure}_{\mathcal{M}}\ \psi\ r$ (measurement)

with appropriate definitions

Formal Analysis of PT Games

To formally reason about pseudo-telepathy games, we formalize them as distributed quantum programs. A *strategy* program S is *winning*, given a *promise* P and a *winning condition* W, if $P \wedge S \Longrightarrow W$.

Example: Mermin's Game



The Promise: $P :== (x_0 + x_1 + x_2) \mod 2 = 0$
The Winning Condition: $W :== (y'_0 + y'_1 + y'_2) = (x_0 + x_1 + x_2)/2 \mod 2$

The corresponding distributed quantum program:

$$S :== \psi := |000\rangle/\sqrt{2} + |111\rangle/\sqrt{2};\ S_0\ ||_\psi\ S_1\ ||_\psi\ S_2$$
$$S_i :== \textbf{if } x_i = 1 \textbf{ then } \psi_i := U\psi_i \textbf{ else } ok; \psi_i := H\psi_i; \textbf{ measure } \psi_i\ y_i$$

where $U|0\rangle = |0\rangle$ and $U|1\rangle = \sqrt{-1} \times |1\rangle$ and $H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $H|1\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$

Proof that the quantum strategy S is winning:

$$\begin{aligned} S &:== \psi := |000\rangle/\sqrt{2} + |111\rangle/\sqrt{2};\ S_0\ ||_\psi\ S_1\ ||_\psi\ S_2 \\ &:== \psi := |000\rangle/\sqrt{2} + |111\rangle/\sqrt{2};\ |(H^{\otimes 3}(U^{x_0} \otimes U^{x_1} \otimes U^{x_2})\psi)\ y'_0 y'_1 y'_2|^2 \times (\psi' = |\mathbf{y}'_0\ \mathbf{y}'_1\ \mathbf{y}'_2\rangle) \\ &:== |H^{\otimes 3}(|000\rangle + (\sqrt{-1})^{x_0+x_1+x_2} \times |111\rangle)/\sqrt{2}\ y'_0 y'_1 y'_2|^2 \times (\psi' = |\mathbf{y}'_0\ \mathbf{y}'_1\ \mathbf{y}'_2\rangle) \\ \sum \psi' \cdot P \times S &:== W \end{aligned}$$

In a classical setting, it is impossible for the three players to have a winning strategy.

Conclusions

The goal of our work is formalizing all aspects of quantum computing, including distributed quantum systems and quantum cryptography. The current state of our research:

what we have done:	what we are doing now:	what we will do next:
• quantum algorithms [3, 4]	• distributed computing	• cryptographic protocols
• quantum non-locality [5]	• quantum communication complexity	• ...

References

[1] Eric C.R. Hehner. *a Practical Theory of Programming*. Springer, New York, first edition, 1993. Current edn. (2007) Available free at www.cs.utoronto.ca/~hehner/aPToP.

[2] Eric C.R. Hehner. Probabilistic predicative programming. In *Proceedings of the 7th International Conference on Mathematics of Program Construction*, volume 3125 of *Lecture Notes in Computer Science*, pages 169–185. Springer, 2004.

[3] A. Tafliovich. Quantum programming. Master's thesis, University of Toronto, 2004.

[4] A. Tafliovich and E.C.R. Hehner. Quantum predicative programming. In *Proceedings of the 8th International Conference on Mathematics of Program Construction*, Kuressaare, Estonia, 2006.

[5] A. Tafliovich and E.C.R. Hehner. Programming telepathy: Implementing quantum non-locality games. In *Proceedings of the 10th Brazilian Symposium on Formal Methods*, Ouro Preto, Brazil, 2007.