Efficient classical verification of quantum computations

Richard Jozsa
and
Sergii Strelchuk

DAMTP, University of Cambridge UK

The issue

Early quantum computer (QC) operating in “high complexity” regime i.e. beyond power of any current classical computers.

How can we establish confidence that its running is correct?

Some possible approaches:

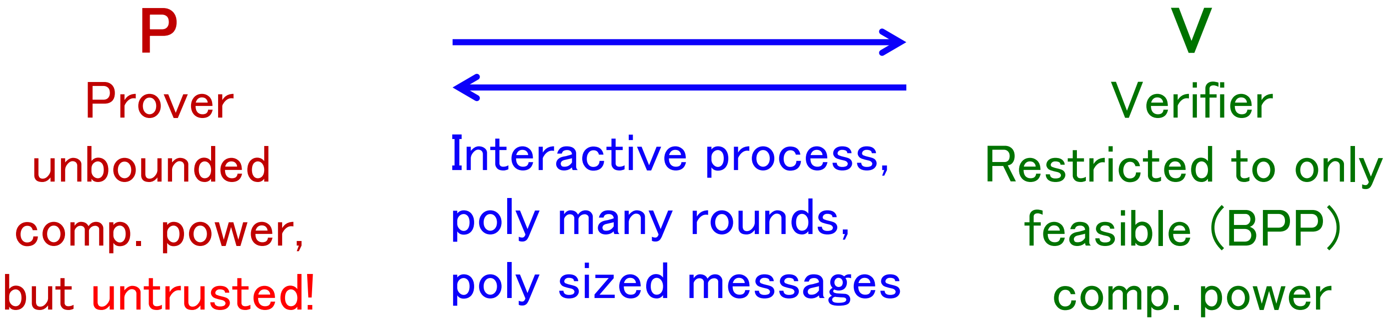
(1) **Classical simulation:** check suitably small QCs (or suitably limited use of QC) by direct classical simulation and statistical tests of the machine.
But want to check beyond this regime!....

(2) NP problems: "solution is computationally hard to get, but if given a candidate solution it is easy to check if it is correct or not" e.g. factoring!

Works well!

But does not apply to general BQP problems (or more general computational tasks like sampling or quantum simulation.)

(3) Methods inspired by theory of interactive proof systems (IP) in classical complexity theory:



P

Prover

unbounded

comp. power,

but untrusted!

Interactive process,

poly many rounds,

poly sized messages

V

Verifier

Restricted to only

feasible (BPP)

comp. power

Decision task: is input x in L? (hard for V to decide!)

Required for IP protocol:

Completeness: if answer is “yes” *and P follows protocol honestly/correctly*
Then Prob(V concludes “yes”) > 1 – eps (any eps > 0)
But don’t trust P to do assigned job honestly/correctly! So:
Soundness: if answer is “no” then for ***any*** P i.e. *honest or dishonest/faulty*,
Prob(V concludes “yes”) < eps
“P cannot trick V into accepting a bad x”

Not symmetric in “yes”/ “no” –
If V concludes “yes” – can be confident that it is correct!
But if V concludes “no” – cannot be confident of result –
need to start over with decision task for complement of L.

Classical theorem:
IP = PSPACE (and a PSPACE prover suffices for protocols).

Can adapt/generalise to quantum setting!

D. Aharonov, M. Ben-or, E. Eban 2008 (then with U. Mahadev 2017).
A. Broadbent 2015.   T. Morimae, J. Fitzsimons 2016.
M. Hayashi, T. Morimae 2015.
Measurement based schemes: J. Fitzsimons, E. Kashefi 2012,
based on A. Broadbent, J. Fitzsimons, E. Kashefi 2008.

QPIP: Quantum Prover Interactive Proofs

∗ P now limited to BQP computing power (i.e. P is our QC machine).
∗ V as before (BPP power) plus some "suitably limited" quantum processing capability.
∗ Completeness and soundness requirements as before.

"Theorem" (various versions): A BQP prover can verify any BQP language to a BPP verifier who also has some (suitably limited, but reliable) quantum processing capability.

Some features of QPIP formalism

(does it solve our verification issue!?)

- Generally don't run original algorithm itself but 'embed' it into a larger algorithm/interaction with inbuilt verification checks (traps for dishonest or faulty P's etc), sometimes also requiring encoded or encrypted states.

- Can question extent of V's quantum capability required
  (can a purely classical V suffice?)

- Do we really need verification against prospectively arbitrarily malicious malfunctioning provers?
  may be suitable for crypto/security issues…
  but not usually demanded in experimental physics/science!?
  Einstein: *"nature hides her secret because of her essential loftiness but not by means of ruse"*.

Some possible approaches (cont)

(4) our approach:

* Novel basis: use results about classically simulatable classes of quantum circuits (and their relation to universal QC) to extend 'verification by classical simulation' techniques to apply to high complexity regime while maintaining poly-scaling of classical verification effort.

* Weaker (more realistic?) demands – verification will not be secure against arbitrarily malicious malfunctioning provers (QCs).

- Can gain in simplicity (fully classical V, QC implements essentially only the original BQP algorithm).
- Have some flexibility to adapt schemes to check/probe particular kinds of suspected sources of failure e.g. specific to an implementational platform.

Our computational scenario

Assume we have –

* QC designed to perform Clifford gates and computational basis measurements.

* Reliable source of various 1–qubit states, including |0>, |1> and magic state |A> = (|0> + $e^{i*pi/4}$ |1>) /√2

Then can implement T = diag (1 $e^{i*pi/4}$) gate by adaptive Clifford process (“T gadget”)

So have universal quantum computing via adaptive Clifford circuits

Theorem:

Let C be any Clifford circuit of size N,
including intermediate measurements, with:
* input being any product state (we'll use only |0>, |1>, |A>)
* one-bit output (i.e. single line final measurement).

Then:

(a) If C is **adaptive** (choice of Clifford gates can depend on earlier intermediate measurement outcomes) then we have universal quantum computing power.

(b) If C is **non-adaptive** then the output probabilities can always be classically efficiently calculated (i.e. in poly(N) time).

Note: (a) involves no new physical processes that do not occur in (b)!

Verifying a BQP computation

* Assume input is |0>···|0>. Express computation as an adaptive Clifford circuit with Prob(output correct) > 0.99999

* Run the adaptive Clifford circuit on the QC. Record the output. Record also the adapted sequence of gates that *actually occurred* – the "computational run".

We assume classical choice of gates is unproblematic!

The QC machine cannot “know” whether the computational run was adaptive or not!!
So QC’s actual physical process (i.e. implementing the gate sequence that occurred) cannot depend on adaptive vs. nonadaptive –ness.
For (reasonable) verification it suffices to verify validity of QC machine’s implementation of ***this*** process.

The adaptive process is universal for BQP but ***after*** any run, the process that *actually occurred* is classically simulatable! – so can comprehensively check it with further runs of the same sequence (run non-adaptively now) and statistical checks against classically efficiently predictable behaviour.

Example of checks

Paulis classically efficiently determined

giving p_+ and p_- values classically efficiently, and then compare statistics of QC's runs. But will often get $p_+ = p_- = ½$.

To further probe correctness of implementation of C, can check the individual Pauli's:
Change input to product state $|p_1\rangle|p_2\rangle..|p_{n+t}\rangle$ where $|p_i\rangle$s are +/− eigenstates of corresponding correct P_i's.
Then Z_1 measurement output is deterministic i.e. Prob(+) or Prob(−) is 1, depending on +/− choices for $|p_i\rangle$s.

Similarly could check Z and X measurements on each line which characterises Clifford C uniquely.

Summary

Efficient classical simulation techniques can be used to verify operation of a QC machine in ‘high complexity’ regime i.e. beyond direct classical simulability.

The verification scheme is not effective against arbitrarily malicious malfunctioning in the QC, but may suffice in many practical situations, in line with common scientific practice.