Title: Chris Cade: Post-selected classical query complexity

Date: Jan 23, 2019 04:00 PM

URL: http://pirsa.org/19010075

Abstract: <p>The precise relationship between post-selected classical and
post-selected quantum computation is an open problem in complexity
theory. Post-selection has proven to be a useful tool in uncovering some
of the differences between quantum and classical theories, in
foundations and elsewhere. This is no less true in the area of
computational complexity -- quantum computations augmented with
post-selection are thought to be vastly more powerful than their
classical counterparts. However, the precise reasons why this might be
the case are not well understood, and no rigorous separations between
the two have been found. In this talk, I will consider the difference in
computational power of classical and quantum post-selection in the
computational query complexity setting.

We define post-selected classical query algorithms, and relate them to
rational approximations of Boolean functions; in particular, by showing
that the post-selected classical query complexity of a Boolean function
is equal to the minimal degree of a rational function with nonnegative
coefficients that approximates it (up to a factor of two). For
post-selected quantum query algorithms, a similar relationship was shown
by Mahadev and de Wolf, where the rational approximations are allowed to
have negative coefficients. Using our characterisation, we find an
exponentially large separation between post-selected classical query
complexity and post-selected quantum query complexity, by proving a
lower bound on the degree of rational approximations to the Majority
function.</p>

Post-selected classical query complexity

Chris Cade
University of Bristol, UK

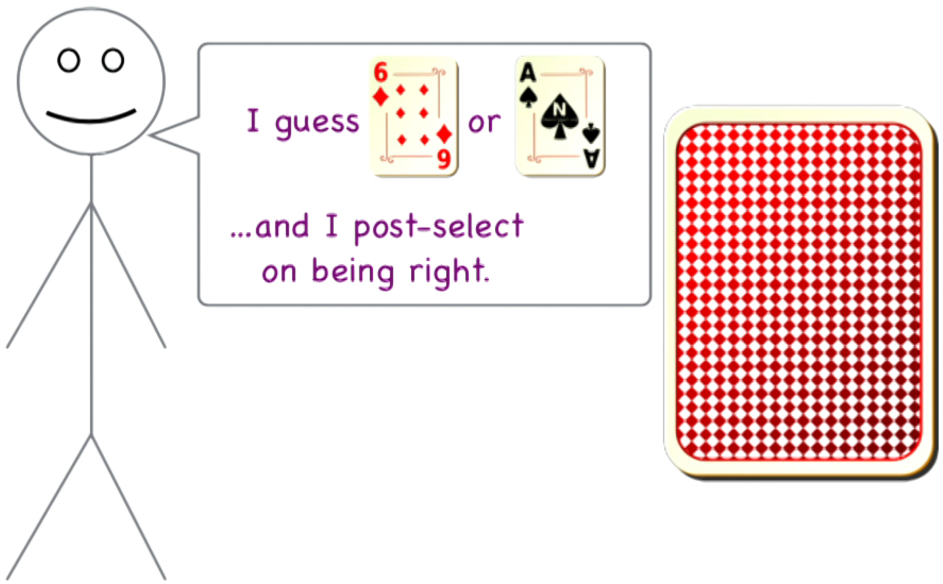
arXiv:1804.10010

EPSRC
Engineering and Physical Sciences
Research Council

University of BRISTOL

Post-selection

The (hypothetical) ability to choose the outcome of a random event

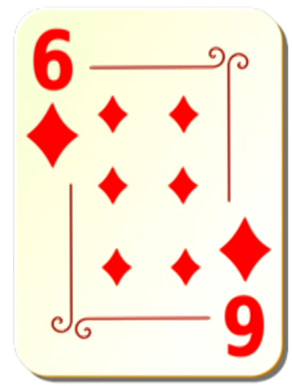


Post-selection

The (hypothetical) ability to choose the outcome of a random event

Post-selection

The (hypothetical) ability to choose the outcome of a random event



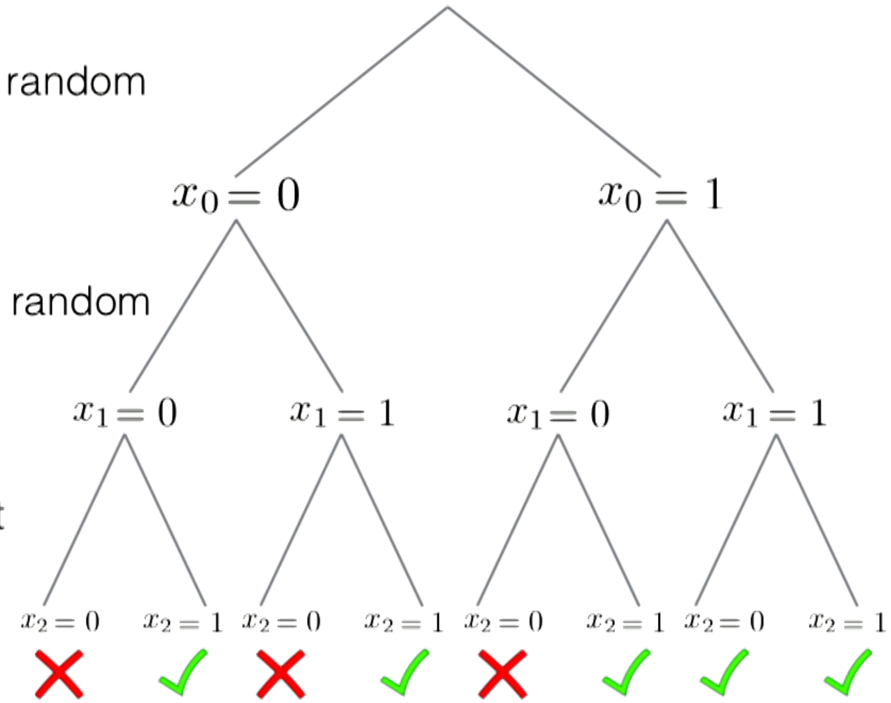
The ability to discard computational paths where some event doesn't occur

$$\boxed{(x_0 \vee x_1 \vee x_2) \wedge (x_0 \vee x_2) \wedge (x_1 \vee x_2) = 1?}$$

1. Choose x_0 at random

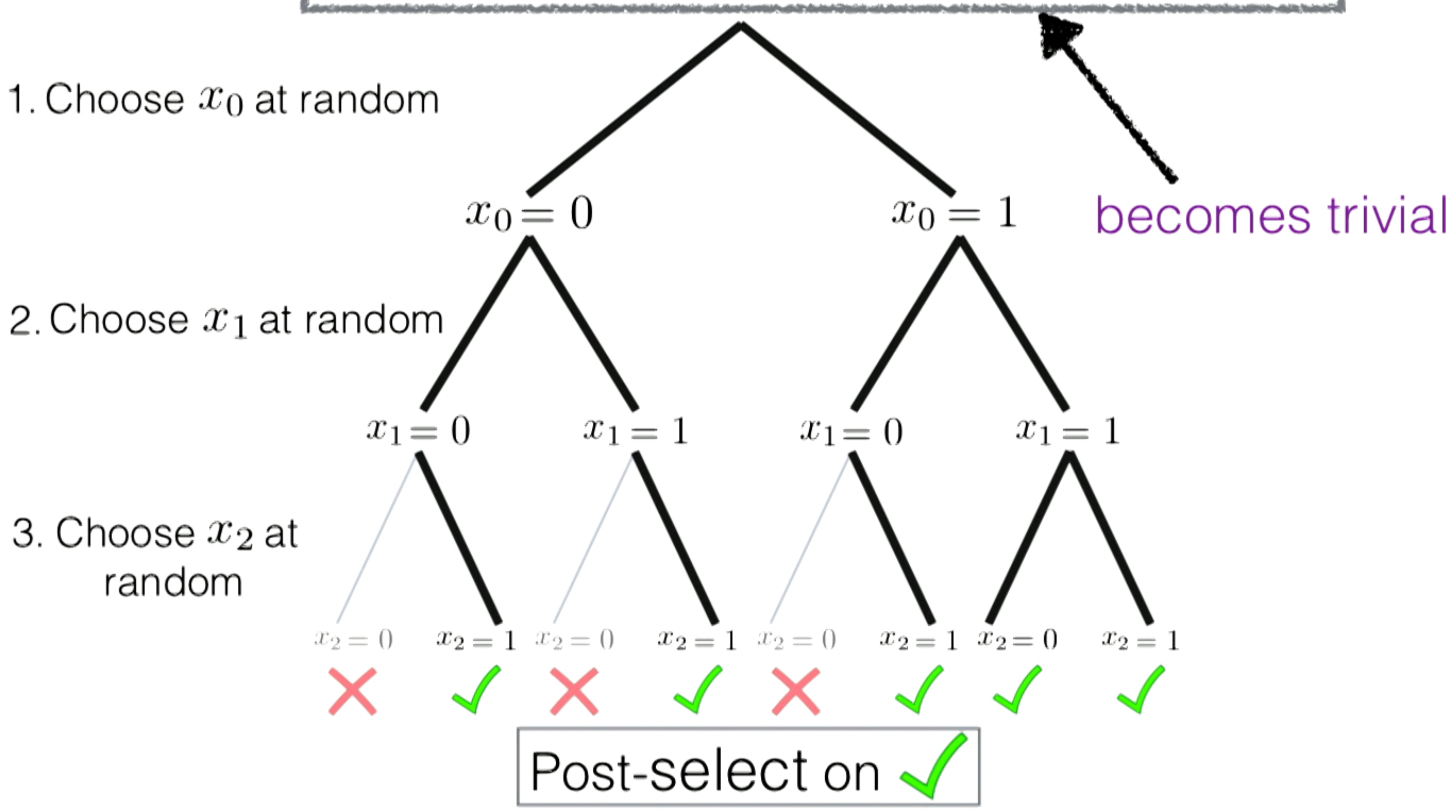
2. Choose x_1 at random

3. Choose x_2 at random



The ability to discard computational paths where some event doesn't occur

$$(x_0 \vee x_1 \vee x_2) \wedge (x_0 \vee x_2) \wedge (x_1 \vee x_2) = 1?$$



- What other problems become easy?
- What happens if we have a *quantum* computer with post-selection?

PostBPP:

Given two randomised (poly-time) algorithms *A* and *B*

$$\text{if } x \in L, \qquad \Pr\left[A(x) = 1 | B(x) = 1\right] \geq 2/3$$
$$\text{if } x \notin L, \qquad \Pr\left[A(x) = 1 | B(x) = 1\right] \leq 1/3$$
$$\Pr[B(x) = 1] > 0$$

PostBQP:

Given two *quantum* (poly-time) algorithms *A* and *B*

$\ldots$

Motivation

- We only know how to prove *polynomial* separations between quantum and classical computation
  - exponential separations are either conjectured, or for partial functions.
- Post-selection exaggerates this difference: we can prove *exponential separations* (this talk).
- Studying the computational power of extensions to quantum mechanics can help to explain why quantum mechanics is the way it is
  - e.g.:
    - non-unitary evolution, measurement probability $|\alpha|^p$ for $p \neq 2$ both allow simulation of post-selection

NP: $\exists x$ s.t $f(x) = 1$?

coNP: $\forall x$ does $f(x) = 1$?

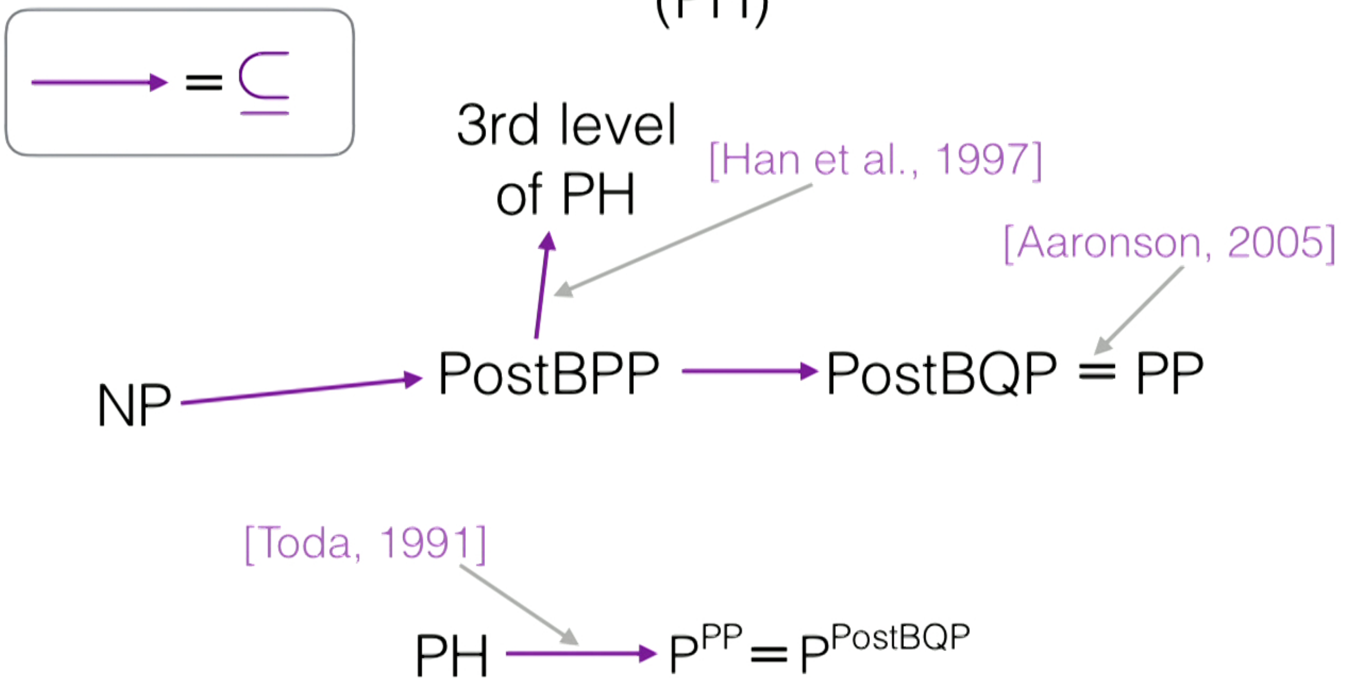
2nd PH : $\exists x$ s.t. $\forall y$, $f(x,y) = 1$?

$\forall x$, $\exists y$ s.t. $f(x,y) = 1$?

$\vdots$

$\exists x$, $\forall y$, $\exists z \ldots$

PostBPP, PostBQP and the Polynomial Hierarchy (PH)



If PostBPP = PostBQP, then the PH collapses to the third level.

Quantum Computational Supremacy

Roughly…

1. If **BPP = BQP**, then **PostBPP = PostBQP**
2. Adding post-selection to non-universal quantum computational models makes them universal, e.g.
    1. One clean qubit, Boson sampling, IQP circuits
3. If these models can be simulated efficiently classically, then **PostBPP = PostBQP**
4. And the **PH** collapses

Query Complexity

- Only count the number of queries we need to make to the input, not the total computation time.
- Why study it? We can actually prove things!
- We can prove separations between the power of quantum and classical computation in the query model
    - e.g. **unstructured search** gives a **quadratic separation**

$$\boxed{\begin{array}{ll} \Theta(N) & \text{classical queries} \\ \Theta(\sqrt{N}) & \text{quantum queries} \end{array}}$$

Post-selected classical query complexity

- PostR : Query analogue of **PostBPP**
- E.g. post-selected query algorithm to compute OR(x)

1. Choose a random index $i \in \{0, \ldots, N-1\}$.
2. If $x_i = 1$, return 1.
3. Else, with probability $\frac{1}{2N}$ return 0.
4. Otherwise, return '**don't know**'.
5. Post-select on *not* seeing '**don't know**'

$\boxed{\text{PostR}(OR) = 1}$

Polynomial Approximation

- An ***N***-variate multilinear polynomial $P : \{0,1\}^N \to \mathbb{R}$

$$P(x) = \sum_{S \subseteq [N]} \alpha_S \prod_{i \in S} x_i$$

- A polynomial P ϵ-approximates a function f if

$$|P(x) - f(x)| \leq \epsilon$$

- The *degree* of a polynomial is the size of its largest monomial

$$deg\ (P) = \max\{|S| : \alpha_S \neq 0\}$$

- The acceptance probability of a ***T*-query** quantum query algorithm can be written as a degree-***2T*** *polynomial.*

$$|\text{state after } T \text{ queries}\rangle = \sum_{z \in \{0,1\}^n} \alpha_z(x) |z\rangle$$

Polynomial of degree T

- Lower bounds on the degrees of polynomials imply lower bounds on quantum query complexity:

$$2 \deg_{\frac{1}{3}}(f) \leq \mathsf{Q}(f)$$

- The "polynomial method" has been used to show many quantum lower bounds
    - e.g. Parity, OR, AND, Majority, Collision problem, etc.

Rational Polynomials and Post-selection

- A *rational polynomial* (or *rational function*) is the ratio of two polynomials:

$$R(x) = \frac{P(x)}{Q(x)}$$

Approximation: $|R(x) - f(x)| \leq \epsilon$

Degree: $\deg(R) = \max\{\deg(P), \deg(Q)\}$

$\mathsf{rdeg}(\mathsf{f})$

- Post-selected quantum query complexity PostQ is characterised by the degree of rational functions: [Mahadev & de Wolf, 2015]

$$\frac{1}{2}\mathsf{rdeg}_\epsilon(f) \leq \mathsf{PostQ}_\epsilon(f) \leq \mathsf{rdeg}_\epsilon(f)$$

Results

- Non-negative rational degree rdeg_ϵ^+ : the polynomials can only have positive coefficients, and are over the variables $x_1, x_2, \ldots, x_N, (1-x_1), (1-x_2), \ldots, (1-x_N)$

- Post-selected *classical* query complexity PostR is characterised by non-negative rational degree

$$\boxed{\mathsf{rdeg}_\epsilon^+(f) \leq \mathsf{PostR}_\epsilon(f) \leq 2\mathsf{rdeg}_\epsilon^+(f)}$$

- Zero-error variant is equivalent to non-deterministic query algorithms:

$$\mathsf{PostR}_0(f) = N(f) = C(f)$$

- Why rational functions?
  - Bayes Theorem: $\Pr[A|B] = \frac{\Pr[B|A]\Pr[A]}{\Pr[B]} = \frac{\Pr[A]}{\Pr[B]}$, where $\Pr[B|A] = 1$

Quantum: [Mahadev & de Wolf, 2015]

$$\frac{1}{2}\mathrm{rdeg}_\epsilon(f) \leq \mathrm{PostQ}_\epsilon(f) \leq \mathrm{rdeg}_\epsilon(f)$$

Coefficients correspond to ***amplitudes***

Can be negative

Classical: [CC, 2018]

$$\mathrm{rdeg}^+_\epsilon(f) \leq \mathrm{PostR}_\epsilon(f) \leq 2\mathrm{rdeg}^+_\epsilon(f)$$

Coefficients correspond to ***probabilities***

Must be positive

Difference between Quantum and Classical? **Probabilities vs. Amplitudes**

Separations

- Using the OR function. $\text{PostR}(OR) = 1$

Quantum	$\text{Q}(OR) = \Theta(\sqrt{N})$
Exact post-selected classical	$\text{PostR}_0(OR) = N$
Quantum Certificate (query analogue of QMA)	$\text{QC}(OR) = \Theta(\sqrt{N})$

- Degree-1 rational polynomial for approximating OR

$$P_{OR}(x) = \frac{\sum_{i=1}^{N} x_i}{\epsilon + \sum_{i=1}^{N} x_i}$$

PostR vs. PostQ

- Majority function on N bits:

$$\mathsf{MAJ}_N(x) = \begin{cases} 1 & \text{if } |x| > N/2 \\ 0 & \text{if } |x| \le N/2 \end{cases}$$

There is no low-degree rational approximation to the Majority function that has nonnegative coefficients.

$$\mathrm{rdeg}^+(\mathsf{MAJ}_N) = \Omega(N)$$

$$\Big\downarrow \ \mathrm{rdeg}^+(f) \le \mathrm{PostR}(f)$$

There is no efficient post-selected classical query algorithm for computing Majority.

$$\mathrm{PostR}(\mathsf{MAJ}_N) = \Omega(N)$$

$$\Big\downarrow \ \mathrm{PostQ}(\mathsf{MAJ}_N) = O(\log N)$$

$$\boxed{\mathrm{PostQ} \ll \mathrm{PostR}}$$

Post-selection amplifies differences between quantum and classical

Without post-selection (total functions)

Quantum $\longleftrightarrow$ Classical (randomised)

Q — Polynomially related — R

Largest known separation: $\mathrm{R}(f) = \tilde{\Omega}(\mathrm{Q}(f)^{2.5})$ [Aaronson et al., 2016]

With post-selection

Quantum $\longleftrightarrow$ Classical

PostQ — **Not** polynomially related — PostR

Largest known separation: $\mathrm{PostR}(f) = \Omega(2^{\mathrm{PostQ}(f)})$ [CC, 2018]

Page 108 of 112

Extras

- The Majority lower bound can be generalised to all symmetric Boolean functions. Analogous to a result of Paturi.

- All lower bounds carry over to the communication complexity setting (via the 'simulation theorem' of Göös et al.)

Summary

- When we add post-selection, we can nicely characterise classical query complexity
- Allows us to directly compare the quantum and classical cases:
  - Exponential separation for the Majority function
  - Difference lies in the use of amplitudes over probabilities
- Post-selection exaggerates the differences between quantum and classical computing