Non-standard Advice Sources for Quantum Computation

Andrew Drucker

MIT

October 2011

- Based on joint works with Scott Aaronson

  ["A Full Characterization of Quantum Advice", STOC '10];

  ["Advice Coins for Classical and Quantum Computation", ICALP '11]

Big picture

- Non-uniform computation: models idea of "preprocessing" or "special hardware" for a fixed input length n.

- Two standard, equivalent formulations (for either classical or quantum poly-time algorithms):

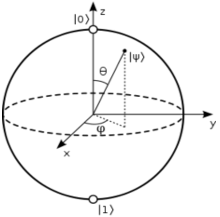
  1. poly(n)-length advice string a_n depending only on input length n;
  2. poly(n)-sized circuit C_n

- Resulting complexity classes: P/poly, BQP/poly

Big picture

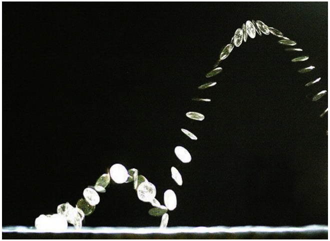
- Both model classical non-uniform advice!
- Other possibilities for quantum algorithms...
- Other models could have more to say about the "effective information content" of quantum systems.

Alternative models



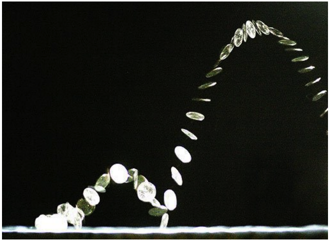
- First natural idea: quantum advice **[Nishimura, Yamakami '03]**
- Length-dependent quantum state $|\psi_n\rangle$, on poly(n) qubits
- Provided to a (uniform) family of poly-sized quantum circuits; measure to get computationally useful info!
- Resulting complexity class: BQP/qpoly

Alternative models



- Second natural (?) idea: advice coins **[E. Demaine]**
- Coin with arbitrary real bias $p_n \in (0, 1)$; flip to reveal computationally useful info!

Alternative models



- Interesting case: space-bounded computation
- Resulting complexity class: BQPSPACE/coin

Our results

- New methods to bound the power of non-standard advice.
- Precise characterizations of BQP/qpoly, BQPSPACE/coin in terms of classes involving classical non-uniform advice only:
   1. BQP/qpoly = a restricted subclass of QMA/poly;
   2. BQPSPACE/coin = PSPACE/poly.

Exploiting special structure in QM

- For each advice type, first step: clarify the object of study.
- Fix a quantum alg. A, input length n,
  and an advice source src (quantum state $|\psi\rangle$ or coin bias p).

  For an input $x \in \{0,1\}^n$, define

  $$P^{src}(x) \;=\; \text{acceptance probability of } A^{src}(x).$$

Exploiting special structure in QM

- Using previous work, we identify collective structure of the functions

$$\{P^{src}(x)\}_{src},$$

as we range over src.

Exploiting special structure in QM

- Not just a "random collection" of functions;

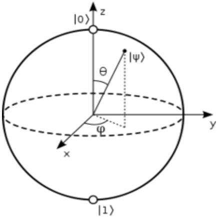
  QM $\Longrightarrow$ strong constraints!

  1. Quantum advice states: $\{P^{|\psi\rangle}(x)\}_{||\psi\rangle| \leq n^c} \; = \;$ a "skinny" (low-dimensional) collection of functions, in an appropriate sense;

  2. Advice coins: $\{P^p(x)\}_{p \in (0,1)} \; = \;$ "algebraically nice" collection.

- Second step: give specific algorithmic techniques to exploit this structure.

Quantum advice states



- **Given:**

$$L \in \mathrm{BQP/qpoly} \quad \longleftrightarrow \quad \{C_n, |\psi_n\rangle\},$$

with $|C_n| = \mathrm{poly}(n)$, $|\psi_n\rangle$ an advice state on n^c qubits.

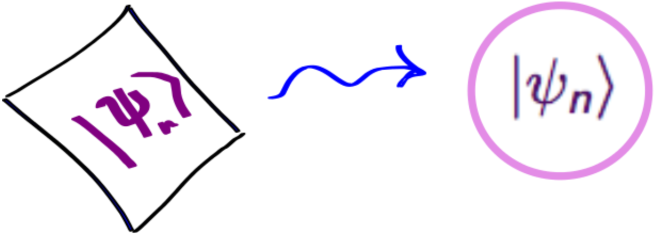
Quantum advice states

- **Given:**

$$L \in \mathrm{BQP/qpoly} \quad \longleftrightarrow \quad \{C_n, |\psi_n\rangle\},$$

with $|C_n| = \mathrm{poly}(n)$, $|\psi_n\rangle$ an advice state on n^c qubits.

- **Ideal goal:** classical description $desc(|\psi_n\rangle)$ that lets us efficiently synthesize a "good-enough copy" of $|\psi_n\rangle$.



Quantum advice states

- Would imply BQP/qpoly $=$ BQP/poly...
- But... don't know how!
- Don't even know how to recognize a copy of $|\psi_n\rangle$ when presented with it!

Quantum advice states

- **Relaxed goal:** Classical description $desc(|\psi_n\rangle)$ to let us efficiently recognize a <u>simulator</u> state $|\psi'_n\rangle$.
- Use $|\psi'_n\rangle$ (indirectly) to simulate $C_n^{|\psi_n\rangle}$.

Quantum advice states

- **Yields:** $L \in \mathrm{QMA/poly}$.
  (**Idea:** have Merlin send $|\psi'_n\rangle$; check it against $desc(|\psi_n\rangle)$; and use it!)
- Merlin here can be oblivious: advice can be chosen independent of the input x.
- In paper we show: $L \in \mathrm{QMA/poly}$ is precisely this restricted subclass of $L \in \mathrm{QMA/poly}$.

Sanity check

- Why should a "good-enough" description of $|\psi_n\rangle$ be possible with $\mathrm{poly}(n)$ bits?

  $\approx 2^{2^n}$ "essentially different" states on n qubits!

- Solution: we only care about measurements performed by small circuits!
- Earlier work **[Aaronson '04, '07]** $\Longrightarrow$

  information-theoretic descriptions with $\mathrm{poly}(n)$ bits.

Quantum advice

- For any $|\psi\rangle$ on n^c qubits, let

$$P^{|\psi\rangle}(x) := \text{ acceptance prob. of } C_n^{|\psi\rangle}(x).$$

Key fact

[Ambainis, Nayak, Ta-Shma, Vazirani '99; Aaronson '07]: *the function collection* $\{P^{|\psi\rangle}\}_{||\psi\rangle|=n^c}$ *has polynomially bounded fat-shattering dimension.*

- (A relative of Holevo's Theorem...)
- Such collections: similar in important respects to a finite collection of size $2^{\text{poly}(n)}$!

Quantum advice

- For the "good" advice $|\psi_n\rangle$, we have:

$$P^{|\psi_n\rangle}(x) \in [0, 1/3] \cup [2/3, 1], \qquad \forall x \in \{0,1\}^n.$$

Say that $|\psi_n\rangle$ is "decisive."

- For <u>any</u> decisive state $|\psi\rangle$, let

$$F^{|\psi\rangle}(x) \ := \ \lfloor P^{|\psi\rangle}(x) \rceil \quad \in \{0,1\}$$

be the "rounded" version of $P^{|\psi\rangle}$.

Quantum advice

- Fat-shattering bound $\Longrightarrow$
  at most $2^{\mathrm{poly}(n)}$ functions $F : \{0,1\}^n \to \{0,1\}$ obtainable in this way!
- Let $\mathcal{F} \;=\;$ this collection.
- Major simplifying assumption: let's pretend that

$$\{P^{|\psi\rangle}\}_{||\psi\rangle| = n^c} \quad = \quad \mathcal{F}.$$

Describing quantum advice classically

- So, given: a collection $\mathcal{F}$ of $2^{\mathrm{poly}(n)}$ Boolean functions.

  (Think of Merlin as sending members of $\mathcal{F}$ as black-boxes!)

- Want to give classical description of the "good" function

$$F^* = \left\lfloor P^{|\psi_n\rangle} \right\rceil \in \mathcal{F},$$

  that helps us compute F^* with Merlin's help.

Isolation

Definition

Say that a function $F \in \mathcal{F}$ is <u>simply-isolatable</u> if,
by specifying values of F on some poly(n) inputs $x^1, \ldots, x^m$,
we can <u>uniquely determine</u> F within $\mathcal{F}$.

$$\boxed{10{*}{*}}$$

$$\mathcal{F} = \left\{ \boxed{1111}\,,\ \boxed{0100}\,,\ \boxed{1000} \right\}$$

Isolation

Definition

Say that a function $F \in \mathcal{F}$ is simply-isolatable if,
by specifying values of F on some $\text{poly}(n)$ inputs $x^1, \ldots, x^m$,
we can uniquely determine F within $\mathcal{F}$.

- If F^* is simply-isolatable, we're done:

  Take classical advice $= \big((x^1, F^*(x^1)), \ldots, (x^m, F^*(x^m))\big)$.

  Lets us recognize F^*, distinguish from other $F \in \mathcal{F}$.

Isolation

- Problem: F^* may not be simply-isolatable!

- Toy example:

$$F^* \equiv 0, \qquad \mathcal{F} = F^* \cup (\text{all } \underline{\text{singleton}} \text{ functions})$$

$$n = 2:$$

$$\boxed{0 \;\; 0 \;\; 0 \;\; 0}$$

$$\boxed{1 \;\; 0 \;\; 0 \;\; 0}$$
$$\boxed{0 \;\; 1 \;\; 0 \;\; 0}$$
$$\boxed{0 \;\; 0 \;\; 1 \;\; 0}$$
$$\boxed{0 \;\; 0 \;\; 0 \;\; 1}$$

Isolation

- Solution:

$$\boxed{0\ \ 0\ \ 0\ \ 0} = MAJ\left(\boxed{1\ \ 0\ \ 0\ \ 0}, \boxed{0\ \ 1\ \ 0\ \ 0}, \boxed{0\ \ 0\ \ 1\ \ 0}\right)$$

- Express F^* as the <u>pointwise majority</u> of simply-isolatable functions!

Majority-certificates

Lemma ("Majority-certificates lemma")

For any collection $\mathcal{F}$ of Boolean n-variate functions (with $|\mathcal{F}| \leq 2^{\mathrm{poly}(n)}$), and any $F^* \in \mathcal{F}$, we can write

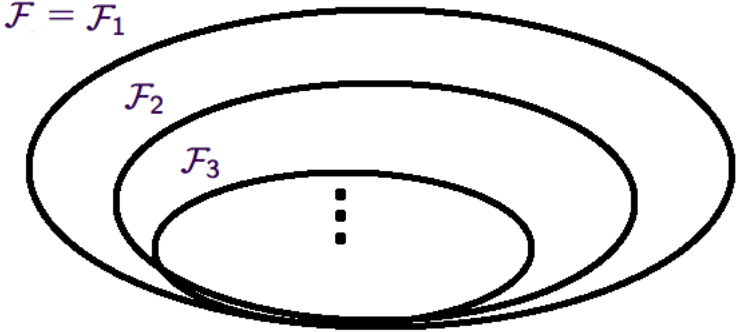
$$F^* \equiv MAJ(\ F_1, \ldots, F_{m=\mathrm{poly}(n)}\ ),$$

where each F_i is simply-isolatable.

- Lets us describe F^* by describing $F_1, \ldots, F_m$.
- Ask Merlin for a copy of $F_1, \ldots, F_m$; check each individually!
- Gives our $\mathsf{QMA/poly}$ protocol for L.

Proof of the majority-certificates lemma

- First, convince ourselves: $|\mathcal{F}| = 2^{\mathrm{poly}(n)} \Longrightarrow \mathcal{F}$ contains at least one simply-isolatable function!
- **Idea:** Take repeated "minority votes".



Proof of the majority-certificates lemma

- Main sub-claim:

Claim

For every distribution $\mathcal{D}$ over inputs $x \in \{0,1\}^n$, there exists an $F \in \mathcal{F}$ that is simply-isolatable, and for which

$$\Pr_{x \sim \mathcal{D}}[F(x) \neq F^*(x)] \ \leq \ 1/10.$$

Proof of the majority-certificates lemma

Claim

For every distribution $\mathcal{D}$ over inputs $x \in \{0,1\}^n$, there exists an $F \in \mathcal{F}$ that is simply-isolatable, and for which

$$\Pr_{x \sim \mathcal{D}}[F(x) \neq F^*(x)] \ \leq \ 1/10. \qquad (**)$$

Proof Sketch.

- Let $x^1, \ldots, x^{m'=\text{poly}(n)}$ be i.i.d. from $\mathcal{D}$.
- If we specify the values $(x^i, F^*(x^i))$, w.h.p. they will be inconsistent with all $F \in \mathcal{F}$ violating (**)!
- On the other hand, they're consistent with <u>some</u> members of $\mathcal{F}$ (e.g., F^* itself). Among these is a simply-isolatable function.

$\square$

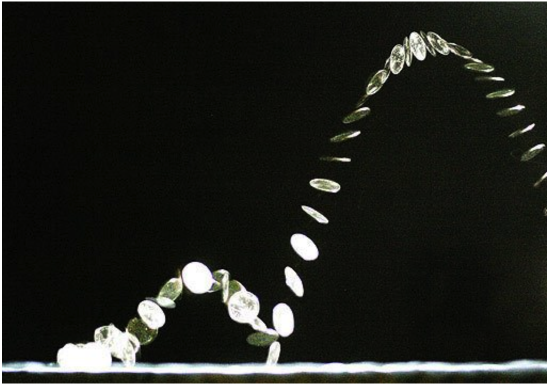
Proof of the majority-certificates lemma

- Next, Minimax Theorem $\implies \exists$ a distribution $\mathcal{D}'$ over simply-isolatable functions $F \in \mathcal{F}$, such that

$$\forall x, \qquad \Pr_{F \sim \mathcal{D}'}[F(x) = F^*(x)] \geq .9.$$

- Our Lemma follows by taking $m = \text{poly}(n)$ samples $F_1, \ldots, F_m \sim \mathcal{D}'$. $\square$

Advice coins



- Coins: a source of randomness.
- But also an information source.
- Flipping a coin, we can learn about coin bias itself!

Advice coins

Definition (Informal)

Let BQPSPACE/coin = set of languages L decidable by a poly-space, quantum Turing machine $A^p(x)$, given access to a non-uniform family of "advice coins" with biases

$$\{p(n)\}_{n>0} ,$$

one bias for each input length n.

- Model details:
  1. Measure at each step to see if A has accepted.
  2. Allowed to reject inputs by running forever.

Our main result

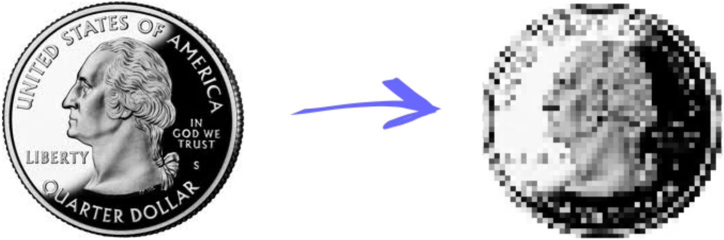
Theorem

$$\mathrm{BQPSPACE/coin} = \mathrm{BQPSPACE/poly}\ .$$

- (Previously known: $\mathrm{BQPSPACE/poly} = \mathrm{PSPACE/poly}$.)
- **Proof sketch:** Let $L \in \mathrm{BQPSPACE/coin}$ be given, solved by $M, \{p(n)\}$...

A first attempt

- Natural idea: simulate a BQPSPACE/coin machine by rounding advice bias to the first poly(n) bits.



- Fails! Machines too sensitive to tiny changes in coin bias.

The "rational behavior" lemma

- Define

$$a_x(p) = (\text{acceptance prob. of } M(x) \text{ on coin bias } p).$$

Lemma

For $p \in (0,1)$, $a_x(p)$ is a rational function in p, of degree $2^{\mathrm{poly}(n)}$.

Coefficients are integers of abs. value $\leq 2^{\mathrm{poly}(n)}$, and computable on demand in PSPACE.

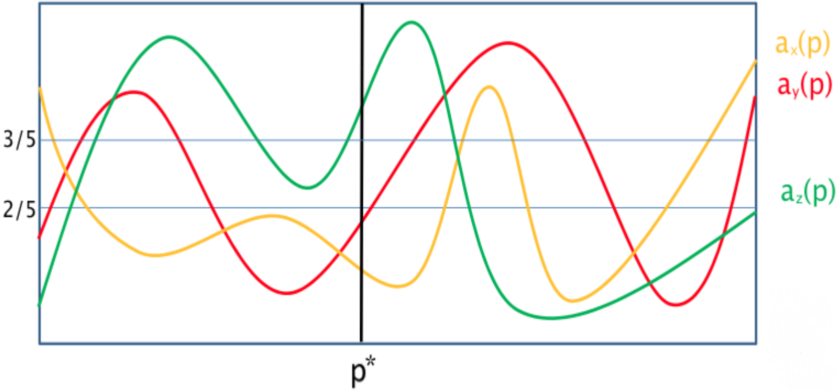
The “rational behavior” lemma

- Proof of the lemma uses a result of **[Aaronson, Watrous ‘09]** to compute limiting behavior of space-bounded computation.
- Uses space-efficient algorithms for matrix inversion.
- Continuity needs to be proved separately—a bit tricky!

Using our lemma

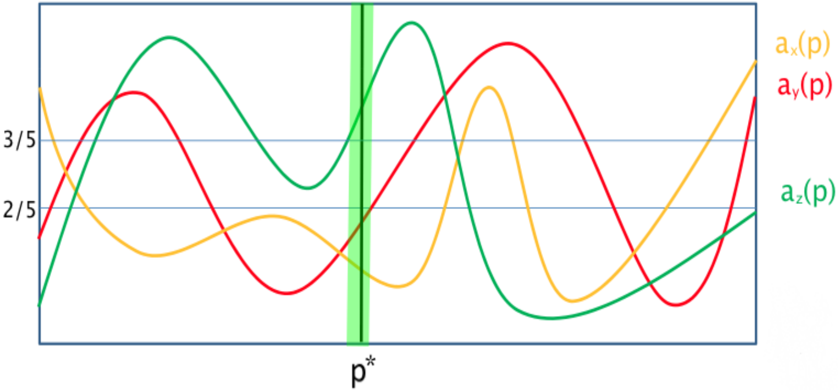
- **Our goal:** use advice to define a "good enough" bias $\tilde{p}$, such that $M^{\tilde{p}}(\cdot)$ decides L_n with $(2/5, 3/5)$-bounded error.
- **Will yield:** $L \in \mathsf{BQPSPACE}/\mathsf{poly}$.

Using our lemma



- **Pictured:** Acceptance probabilities as fcn. of p, for every length-n input.
  $p^* = p(n)$ is the "good" advice bias.

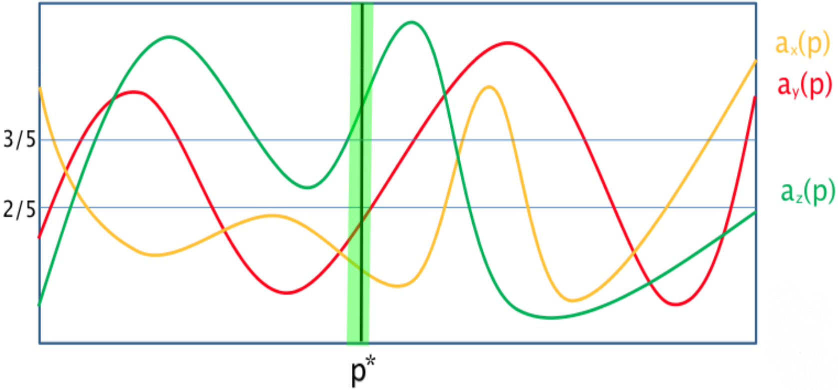
Using our lemma



- Enough to obtain $\tilde{p}$ in interval above!
- Idea: let advice string $a_n =$ number of crossings of $(2/5, 3/5)$-lines lying to the left of p^*.

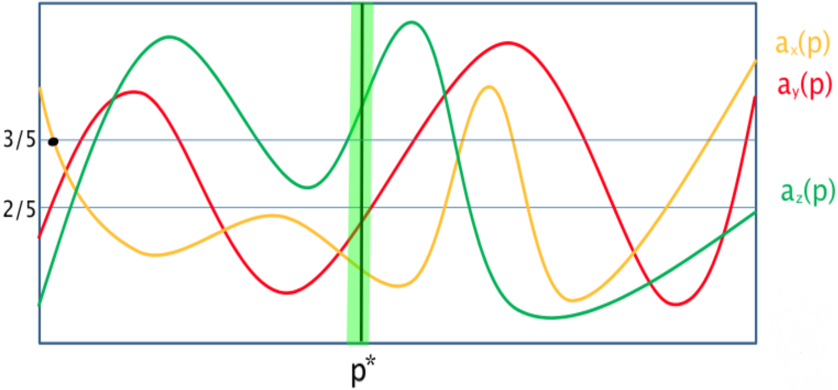
  (At most $2^{\text{poly}(n)}$, so poly-sized advice!)

Using our non-uniform advice



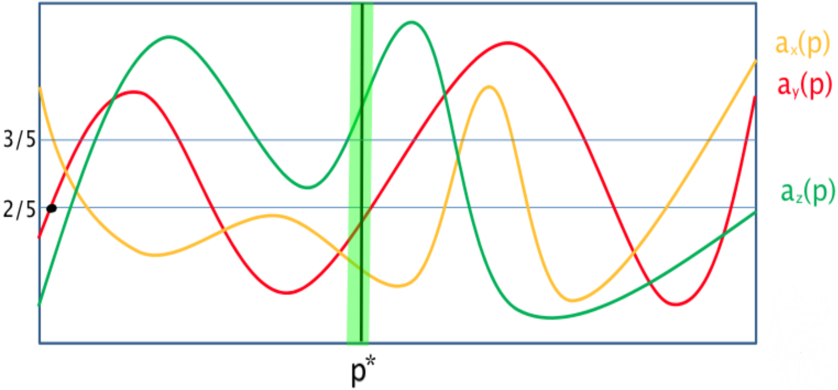
- Wonderful fact: can enumerate these crossings in increasing order, in PSPACE!
- Application of polylog-space algorithm for root isolation of univariate polynomials **[Neff '94]**.

Using our non-uniform advice



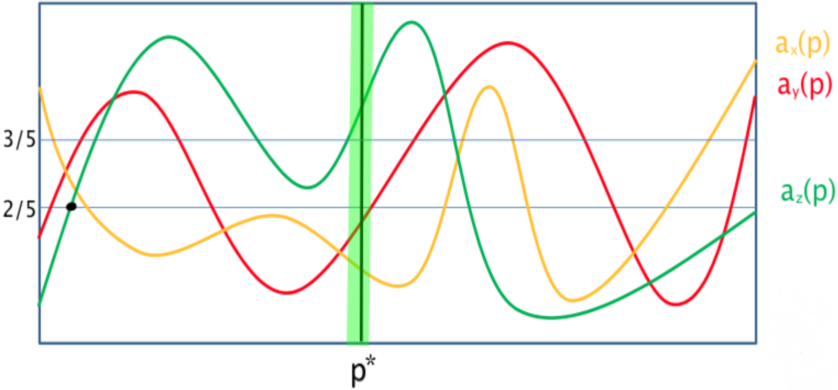
- Wonderful fact: can enumerate these crossings in increasing order, in PSPACE!
- Application of polylog-space algorithm for root isolation of univariate polynomials **[Neff '94]**.

Using our non-uniform advice



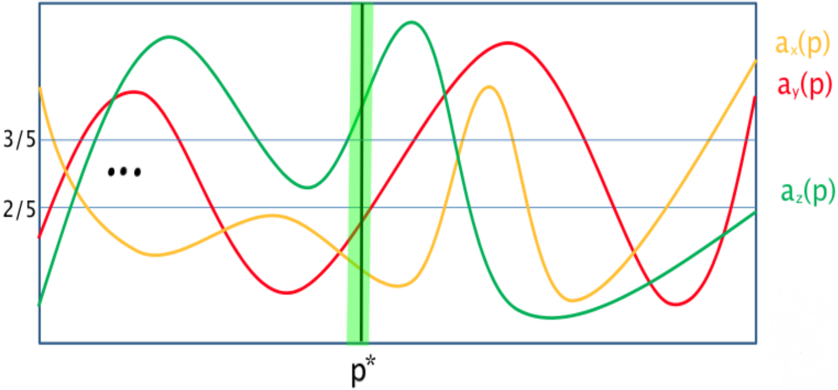
- Wonderful fact: can enumerate these crossings in increasing order, in PSPACE!
- Application of polylog-space algorithm for root isolation of univariate polynomials **[Neff '94]**.

Using our non-uniform advice



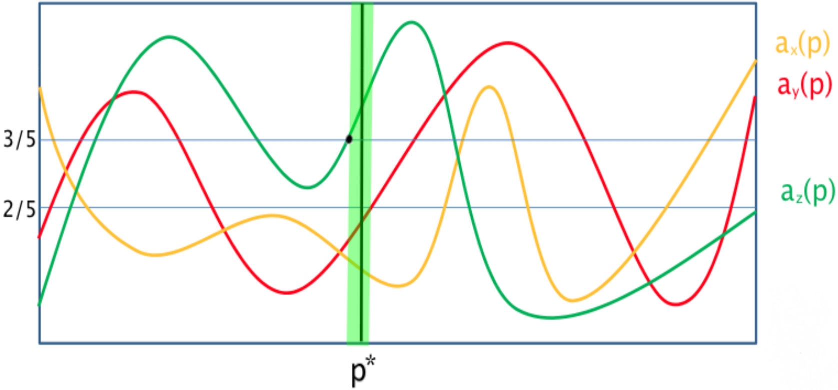
- Wonderful fact: can enumerate these crossings in increasing order, in PSPACE!
- Application of polylog-space algorithm for root isolation of univariate polynomials **[Neff '94]**.

Using our non-uniform advice



- Wonderful fact: can enumerate these crossings in increasing order, in PSPACE!
- Application of polylog-space algorithm for root isolation of univariate polynomials **[Neff '94]**.

Using our non-uniform advice



- Wonderful fact: can enumerate these crossings in increasing order, in PSPACE!
- Application of polylog-space algorithm for root isolation of univariate polynomials **[Neff '94]**.

Using our non-uniform advice

- Remaining challenge: distinct crossings z, z' can be very close together.
- But, not too close: known root-separation bounds for integer polynomials imply
$$|z - z'| \geq 2^{-2^{\mathrm{poly}(n)}} .$$

Using our non-uniform advice

- This is enough to define our $\tilde{p}$:
  with Neff algorithm, we can compute any desired i^{th} bit of a crossing point, up to $i = 2^{\mathrm{poly(n)}}$, in $PSPACE$!
- With this ability, can implement a $\tilde{p}$-biased coin flip, and simulate $M^{\tilde{p}}(x)$.

Open questions

- What's the power of BQPSPACE machines with more than 1 coin?
  Or, with "biased k-sided dice", for $k > 2$?
  We think our techniques can shed light.

- Is $\mathrm{BQP/qpoly} = \mathrm{BQP/poly}$?

- Power of quantum algs. with other unconventional information sources?