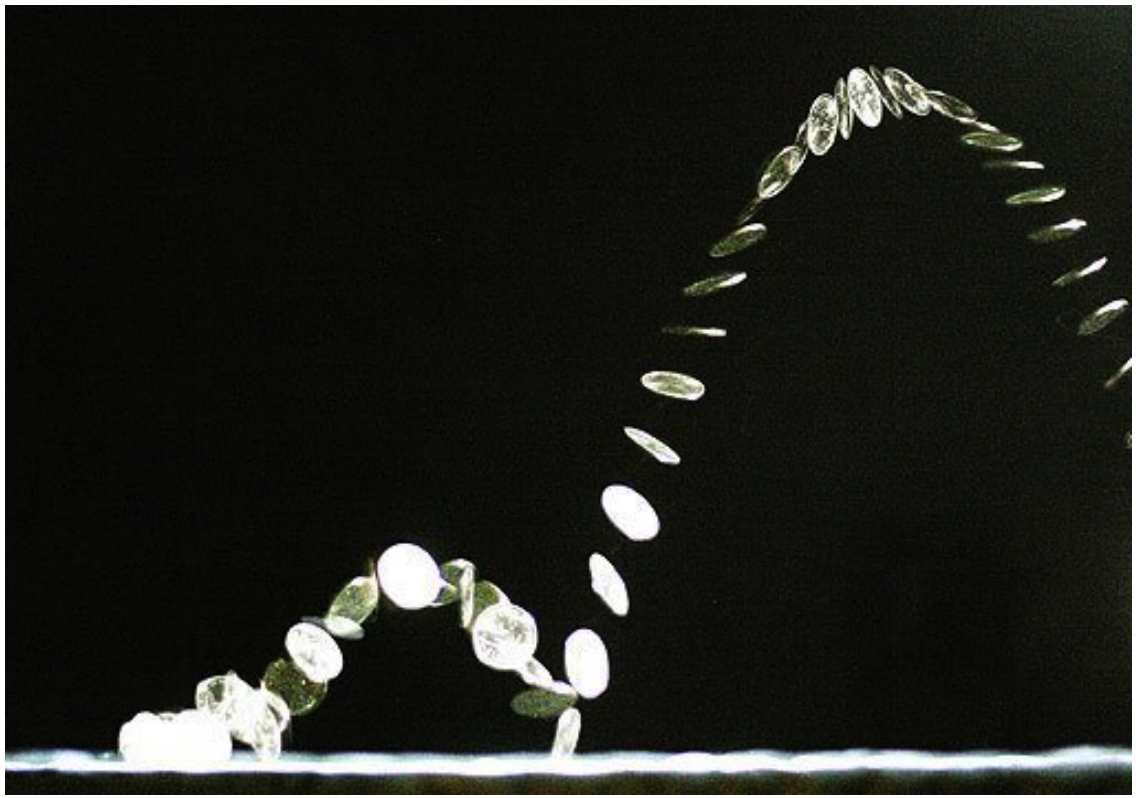
Advice Coins for Classical and Quantum Computation

Andrew Drucker

Joint work with Scott Aaronson

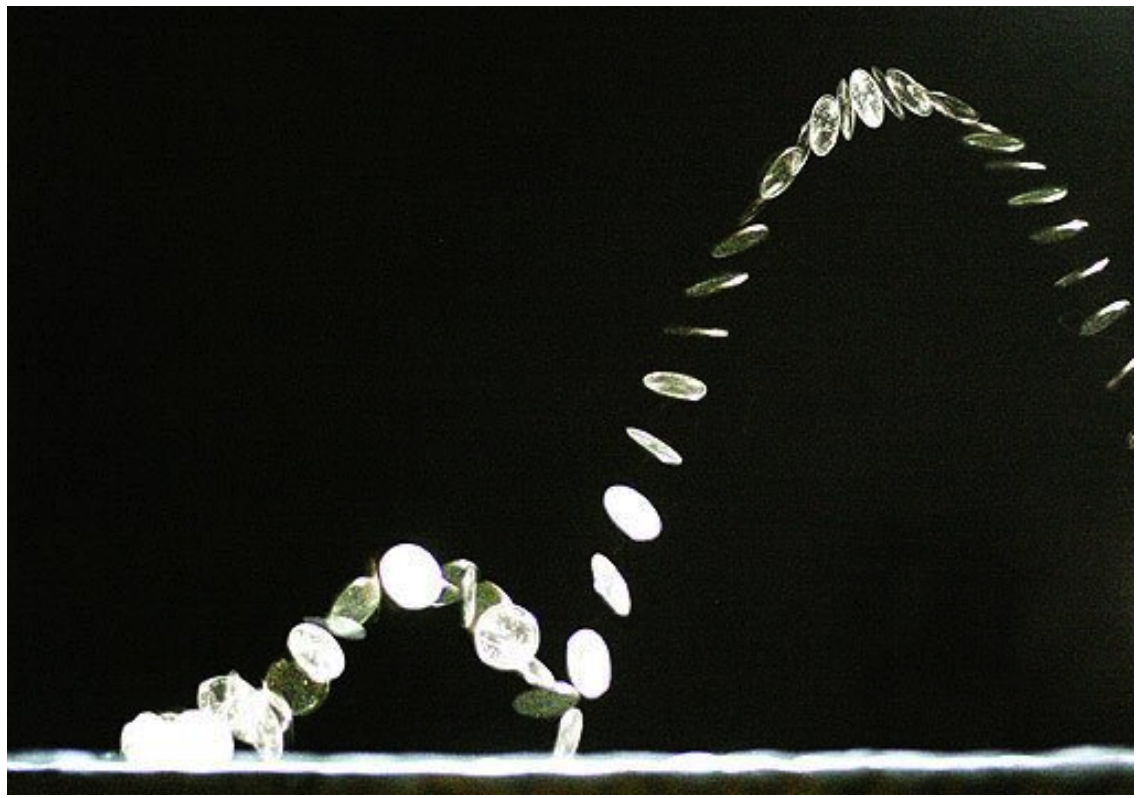
July 4, 2011

Big picture



- Coins: a source of randomness.
  (Valuable in TCS!)

Big picture



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

Big picture

We ask:

- how accessible is this info to efficient coin-flipping algorithms?
- how does the answer change when our algorithms are quantum?

Finding a coin bias

- Say we're given a coin $\$_{p^*}$ of unknown bias $p^* \in [0,1]$.
- Focus on simplest case: assume that

$$p^* \in \{p, p+\varepsilon\}$$

  for known values p, ε.
- Which one is it?

Finding a coin bias

- Sample complexity of this task well-studied in statistics.
- Our focus: what are the space requirements for this task?

The Hellman-Cover Theorem

Theorem (Hellman, Cover '70)

(Classical) probabilistic coin-flipping automata require

$$\Theta\left(\frac{p(1-p)}{\varepsilon}\right)$$

states to distinguish between the cases

$$p^* = p, \quad p^* = p + \varepsilon$$

with bounded error.

The quantum case

- Quantum coin-flipping automata: defined by two evolution superoperators

$$\mathcal{E}_0, \quad \mathcal{E}_1$$

  on the state space;
- On coin bias p, automaton evolves according to

$$p\mathcal{E}_1 + (1-p)\mathcal{E}_0.$$

The quantum case

We show: with quantum algorithms, can do much better:

Theorem

For any p, ε, there is a quantum coin-flipping automaton $A_{p,\varepsilon}$ with just two states (plus accept/reject states), whose acceptance probabilities on the biases

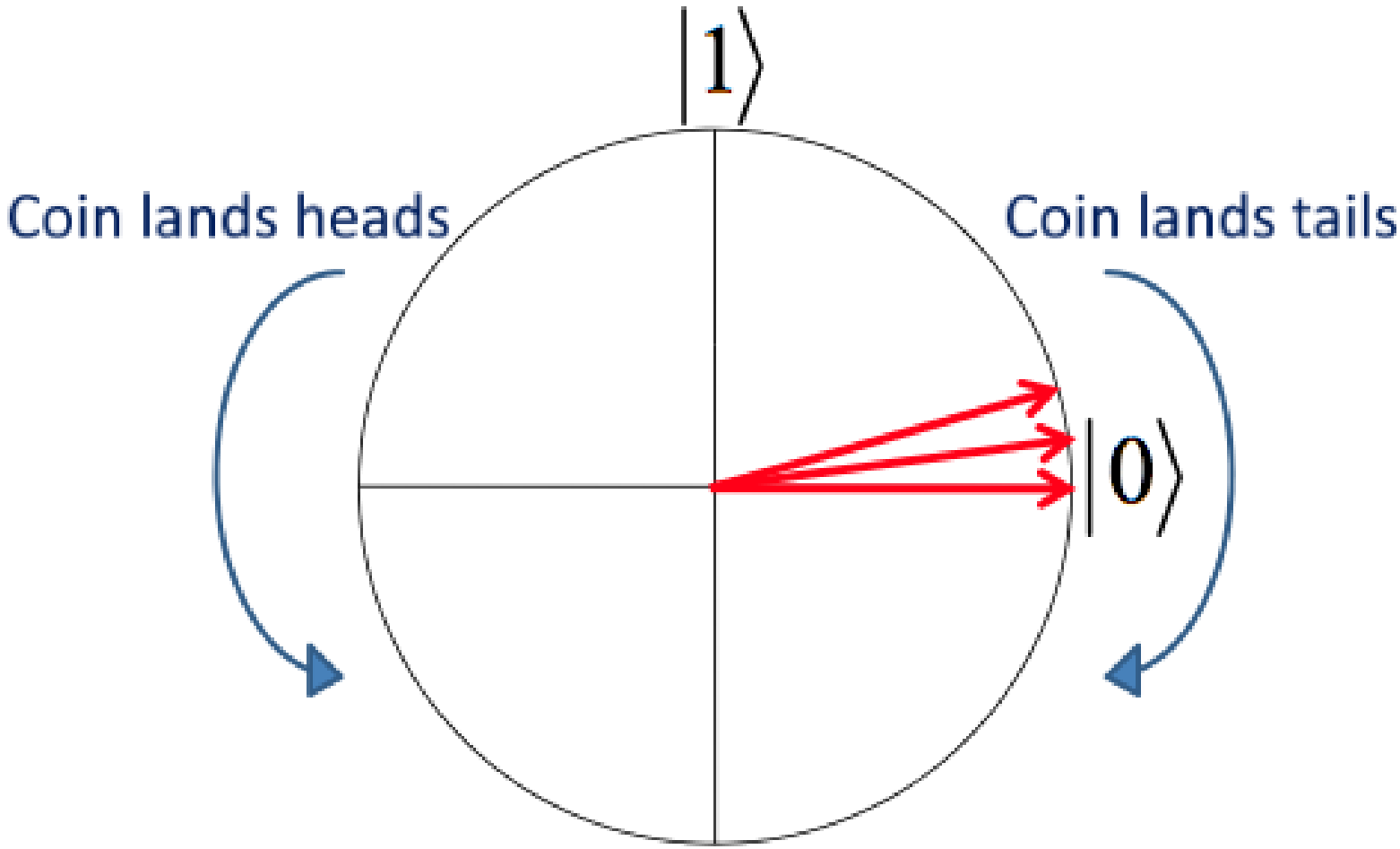
$$p^* = p, \quad p^* = p + \varepsilon$$

differs by at least .01*.*

- **Caveats:**
  1. Transition amplitudes defined in terms of p, ε.
  2. Guarantee breaks down in the presence of noise.

The quantum automaton

- Basic idea: use a qubit as an "analog counter" to perform a random walk.



The quantum automaton

- Each step: measure qubit with probability $\approx \varepsilon^2/10000$.
  $\Longrightarrow$ expect to measure in $O(\varepsilon^{-2})$ steps.

- Rotation amounts designed so that:
  1. $p^* = p$ $\Longrightarrow$ random walk unbiased;
  2. $p^* = p + \varepsilon$ $\Longrightarrow$ random walk has slight c.c. bias.

- Difference in two cases becomes noticeable in $O(\varepsilon^{-2})$ steps!

Coins and quantum computation

- Upshot: space-bounded quantum algorithms can be sensitive to extremely small changes in a coin's bias!
- $\Rightarrow$ Crazy question **[E. Demaine]**: can we store computationally useful information in a coin's bias?
- Coins as new form of nonuniform advice in complexity theory?

Coins as advice

Definition (Informal)

For a complexity class C, let C/coin denote the set of languages L decidable by a C machine, given access to a nonuniform family of "advice coins"

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

one bias for each input length n.

- Modeled on C/poly: languages decidable by C machines augmented with poly-sized nonuniform classical advice string a_n.

Coins as advice

- Most interesting case: space-bounded computation.
- BQPSPACE/coin: bounded-error polynomial-space quantum algs. with advice coins.
- Allowed to run forever with positive probability, and to reject inputs this way.
- Could be a very powerful class....

  Certainly BQPSPACE/coin $\supseteq$ BQPSPACE/poly.

Our main result

Theorem

Actually,

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

- (Previously known: $\mathrm{BQPSPACE/poly} = \mathrm{PSPACE/poly}$.)

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.

A better idea

- Fix a language L, and a BQPSPACE/coin machine $(M, \$_{p(n)})$ for L.
- First, understand how acceptance probability behaves as we vary the advice coin bias!

The "rational behavior" lemma

- Define

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

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

Coefficients are integers of abs. value $\leq 2^{\text{poly}(n)}$, 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.

The "rational behavior" lemma

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

- $*$ Except, possibly, at zeros of denominator!

A continuity lemma

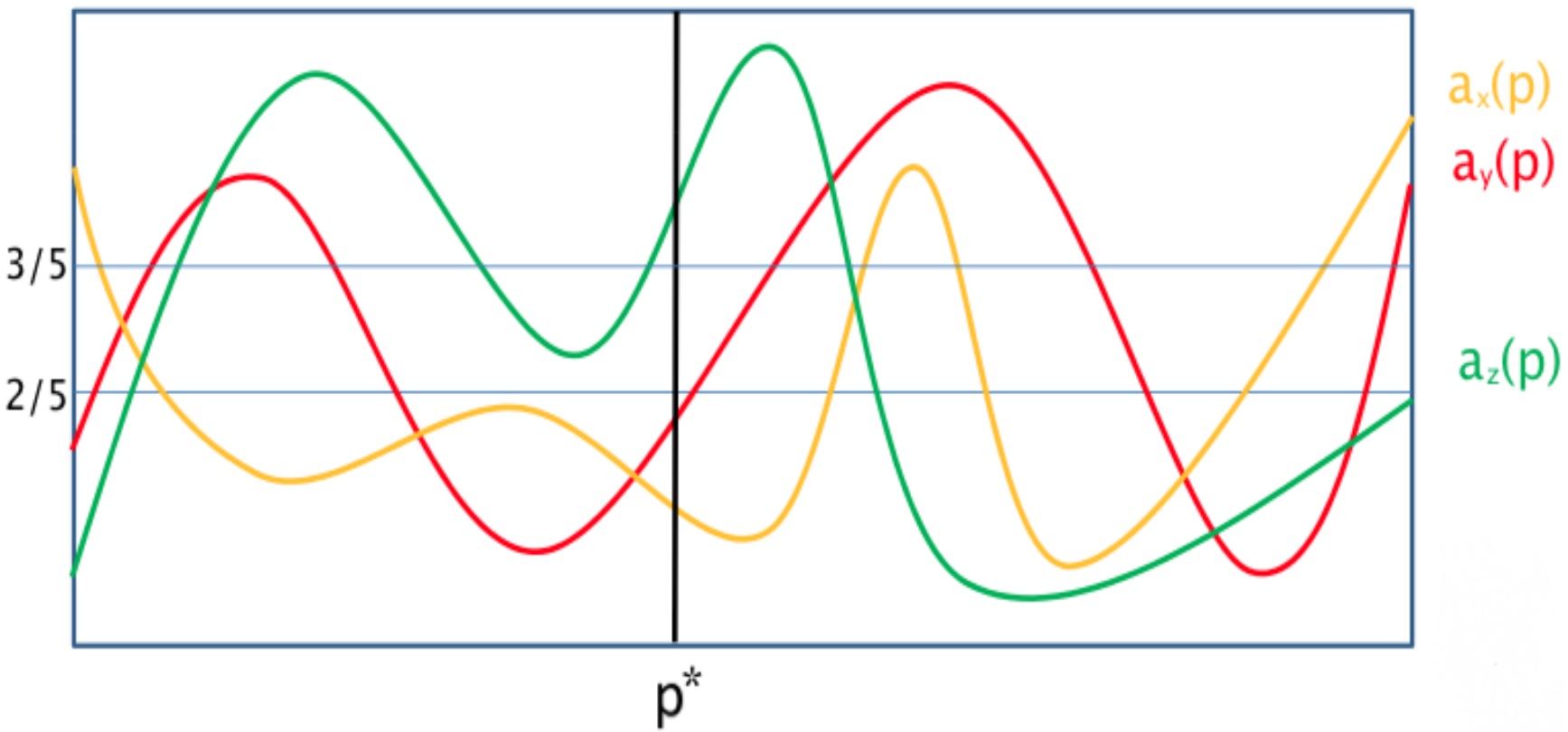
- Need to "patch up" the singularities:

Lemma
$a_x(p)$ *is* *continuous* *for* $p \in (0, 1)$.

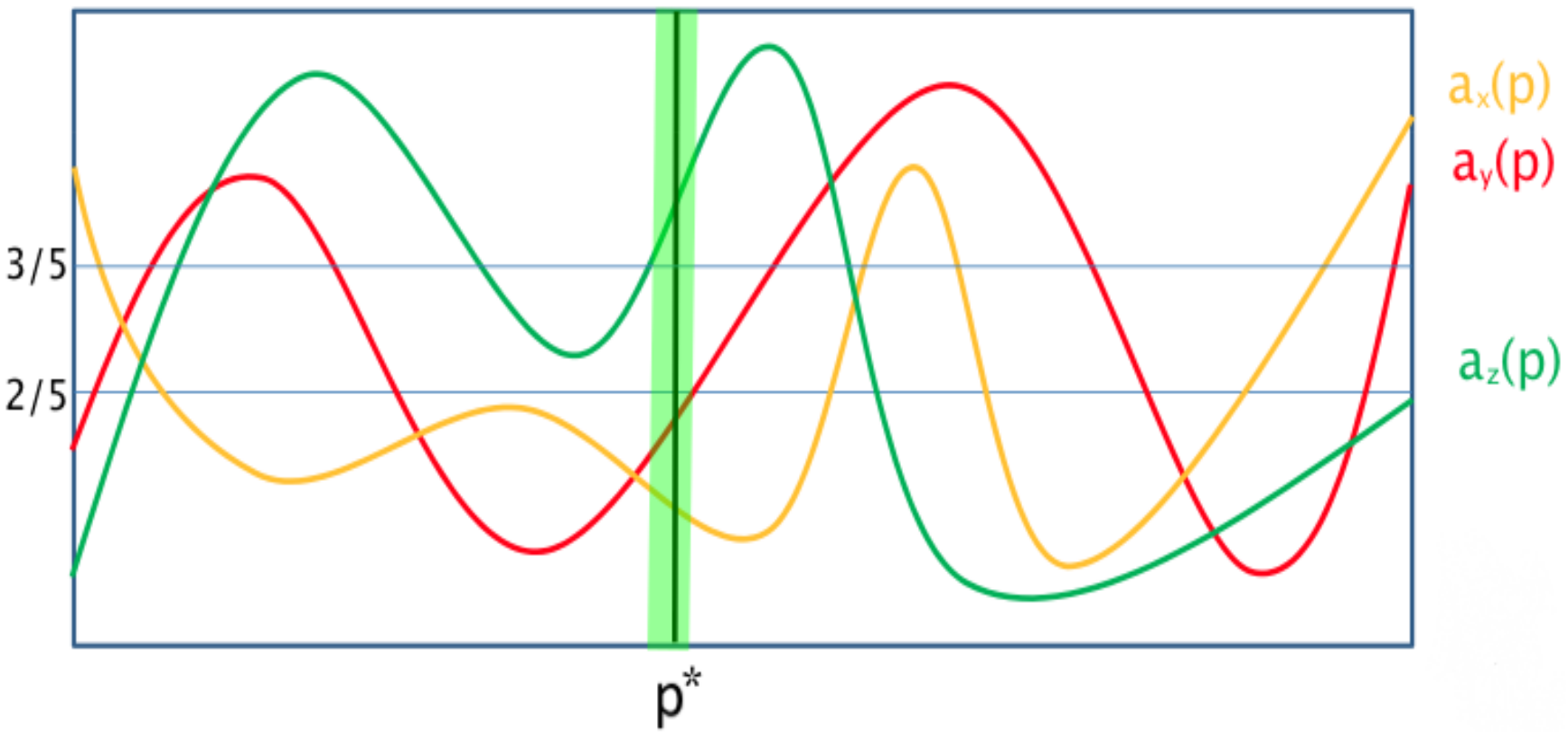
Using our lemmas

- Our goal: obtain a "good enough" bias $\tilde{p}$, such that $(M, \$_{\tilde{p}})$ decides L_n with $(2/5, 3/5)$-bounded error.

Using our lemmas



Using our lemmas

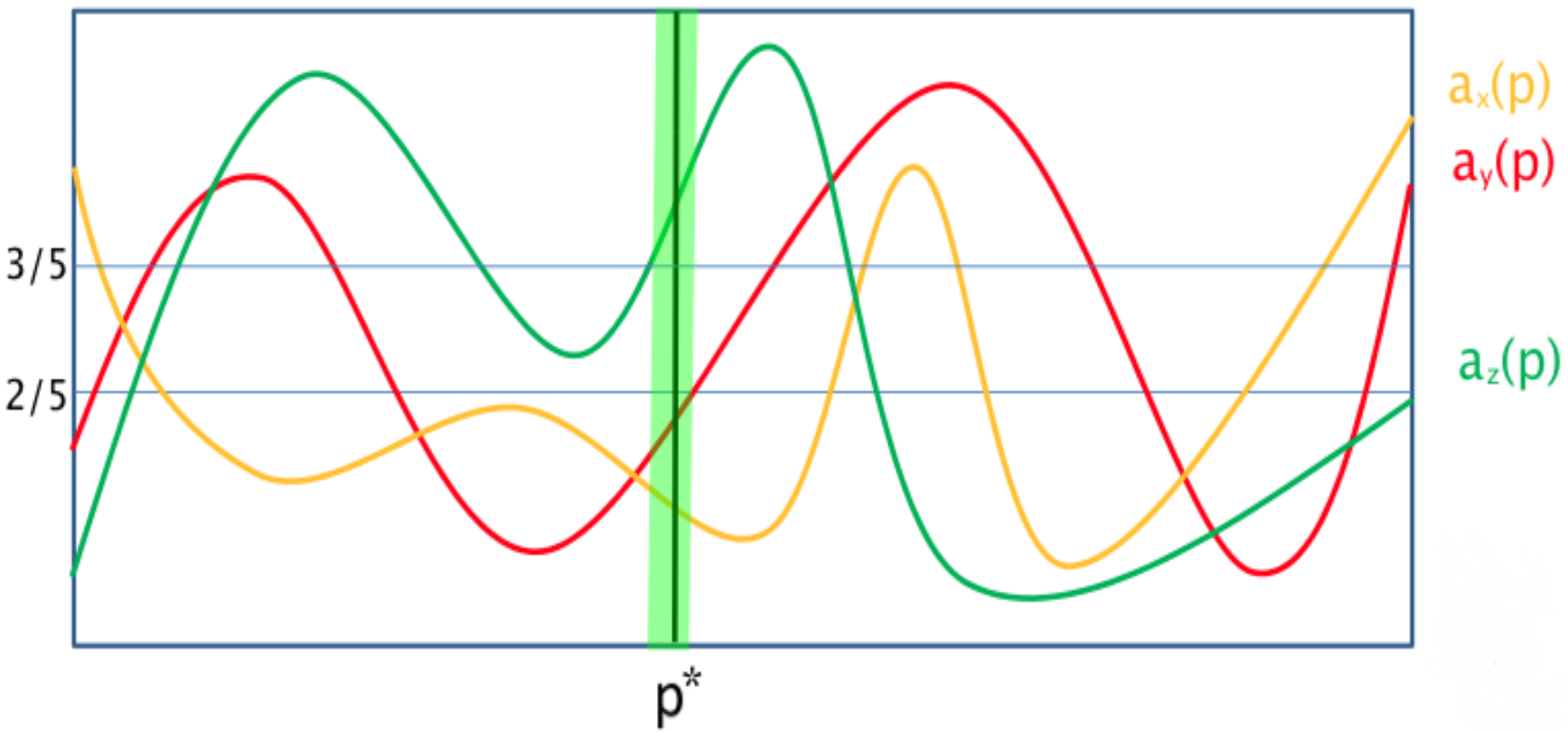


Using our lemmas

- Suffices to find $\tilde{p}$, such that there are no zeros of

$$F_x(p) := (a_x(p) - 2/5)(a_x(p) - 3/5)$$

between p^* and $\tilde{p}$, for any $x \in \{0,1\}^n$.



Using our lemmas

- Idea: let advice string a_n = (number of roots of $\{F_x(p)\}_{|x|=n}$ lying below p^*.
- Only need poly(n) advice bits for this.

Using our nonuniform advice

- Wonderful fact: can enumerate zeros of $\{F_x(p)\}_{|x|=n}$ in increasing order, in PSPACE!
- Application of NC algorithms for root isolation of univariate polynomials **[Neff '94]**.

Using our nonuniform advice

- Remaining challenge: distinct roots z, z' of $\{F_x(p)\}_{|x|=n}$ can be very close together.

- But, not too close: known root-separation bounds for polynomials imply

$$|z - z'| \geq 2^{-2^{\text{poly}(n)}} .$$

Using our nonuniform advice

- This is enough to define our $\tilde{p}$: with Neff algorithm, we can compute any desired i^{th} bit of roots, up to $i = 2^{\mathrm{poly(n)}}$, in *PSPACE*!

- With this ability, can implement a $\tilde{p}$-biased coin flip, and simulate $M(x, \$_{\tilde{p}})$.

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

Thanks!