THE QUANTUM BERNOULLI FACTORY

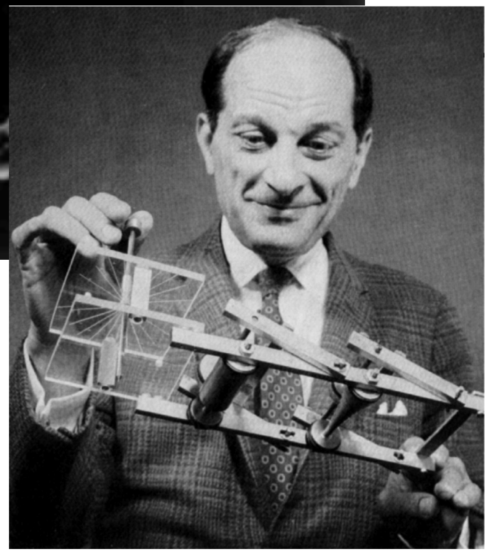
Terry Rudolph

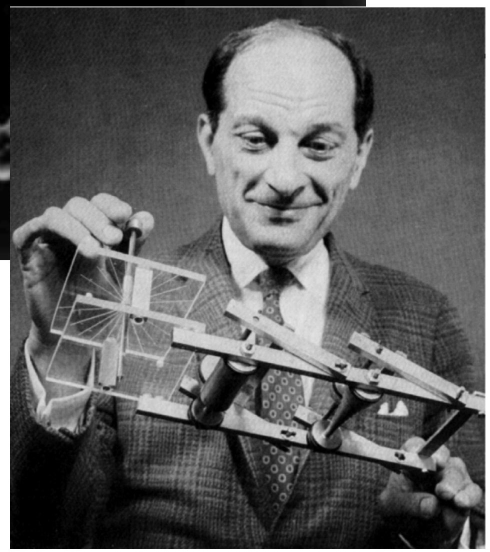
1. arXiv:1509.06183 [pdf, other]

Provable Quantum Advantage in Randomness Processing

Howard Dale, David Jennings, Terry Rudolph

Comments: A much improved version of the paper is available in Nature Communications. (10.1038/ncomms9203)





90's – Invasion of the Math Lords

Invasion I

Provably rapidly mixing
Markov chains

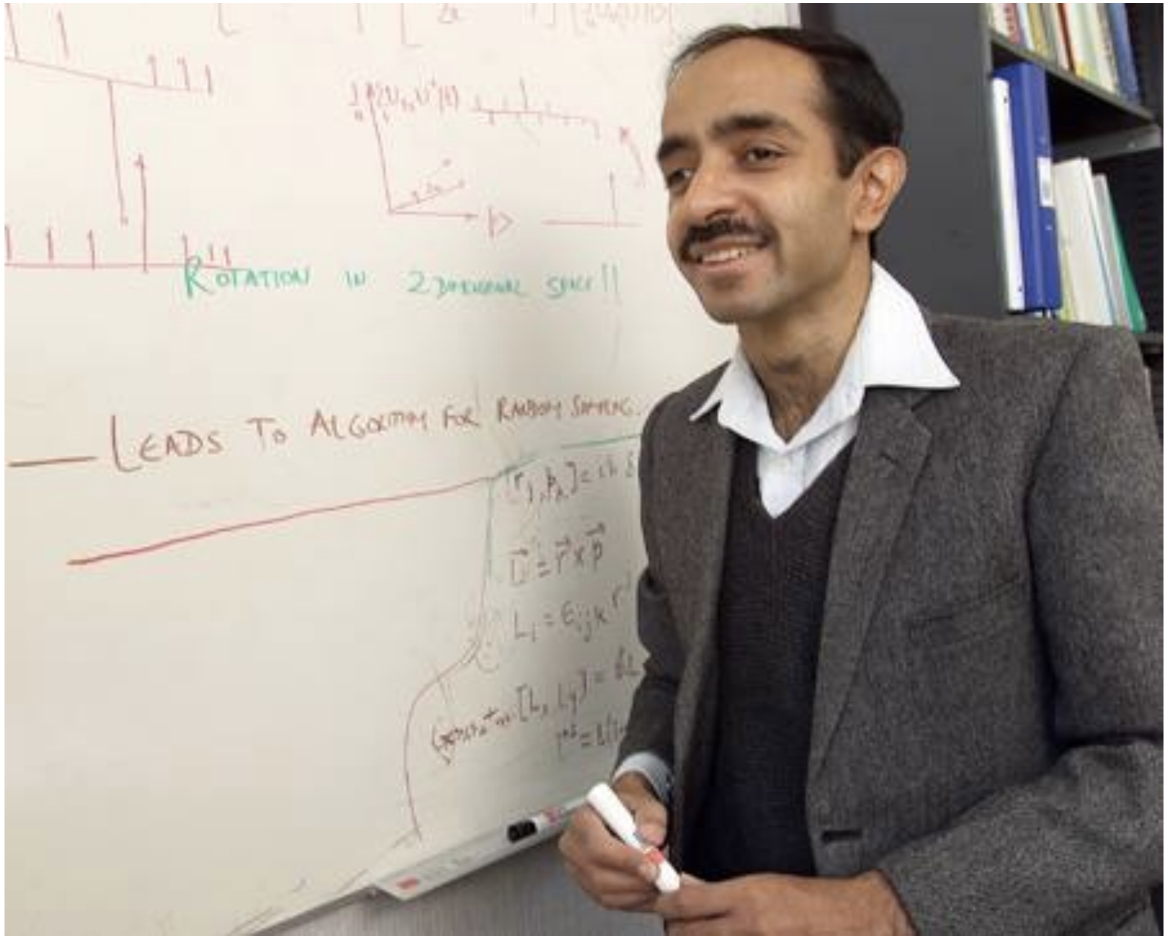
-permanents of +'ve matrices
-integrating log-concave functions
-volumes of convex bodies
-ferromagnetic Ising
(Jerrum, Sinclair, Vigoda, Applegate, Kannan, Dyer, Frieze,...)

90's – Invasion of the Math Lords

Invasion I
Provably rapidly mixing
Markov chains

- -permanents of +'ve matrices
- -integrating log-concave functions
- -volumes of convex bodies
- -ferromagnetic Ising

(Jerrum, Sinclair, Vigoda, Applegate, Kannan, Dyer, Frieze,...)



90's – Invasion of the Math Lords

Invasion I
Provably rapidly mixing
Markov chains

-permanents of +'ve matrices
-integrating log-concave functions
-volumes of convex bodies
-ferromagnetic Ising
(Jerrum, Sinclair, Vigoda, Applegate, Kannan, Dyer, Frieze,...)

i'th configuration $\Omega_i = b_i^1 \ldots b_i^n$ has probability $P(b_i^1 \ldots b_i^n)$

Self Reducible: Efficiently calculate $P(b_i^n = 0 | b_i^1 \ldots b_i^{n-1})$

90's – Invasion of the Math Lords

Invasion I
Provably rapidly mixing Markov chains

- -permanents of +'ve matrices
- -integrating log-concave functions
- -volumes of convex bodies
- -ferromagnetic Ising

(Jerrum, Sinclair, Vigoda, Applegate, Kannan, Dyer, Frieze,...)

$$\text{i'th configuration } \Omega_i = b_i^1 \ldots b_i^n \text{ has probability } P(b_i^1 \ldots b_i^n)$$

$$\text{Self Reducible: Efficiently calculate } P(b_i^n = 0 | b_i^1 \ldots b_i^{n-1})$$

arXiv.org > quant-ph > arXiv:quant-ph/0208112

Quantum Physics

Creating superpositions that correspond to efficiently integrable probability distributions

Lov Grover, Terry Rudolph

90's – Invasion of the Math Lords

Invasion I
Provably rapidly mixing
Markov chains

-permanents of +'ve matrices
-integrating log-concave functions
-volumes of convex bodies
-ferromagnetic Ising
(Jerrum, Sinclair, Vigoda, Applegate, Kannan, Dyer, Frieze,...)

i'th configuration $\Omega_i = b_i^1 \ldots b_i^n$ has probability $P(b_i^1 \ldots b_i^n)$

$$\sum_i \sqrt{P(b_i^1 \ldots b_i^{n-1})} |b_i^1 \ldots b_i^{n-1}\rangle$$

90's – Invasion of the Math Lords

Invasion I

Provably rapidly mixing Markov chains

-permanents of +'ve matrices
-integrating log-concave functions
-volumes of convex bodies
-ferromagnetic Ising
(Jerrum, Sinclair, Vigoda, Applegate, Kannan, Dyer, Frieze,...)

$$\text{i'th configuration } \Omega_i = b_i^1 \dots b_i^n \text{ has probability } P(b_i^1 \dots b_i^n)$$

$$\sum_i \sqrt{P(b_i^1 \dots b_i^{n-1})}|b_i^1 \dots b_i^{n-1}\rangle \left[\sqrt{P(b_i^n = 0|b_i^1 \dots b_i^{n-1})}|0\rangle + \sqrt{P(b_i^n = 1|b_i^1 \dots b_i^{n-1})}|1\rangle\right]$$

90’s – Invasion of the Math Lords

Invasion I
Provably rapidly mixing
Markov chains

-permanents of +’ve matrices
-integrating log-concave functions
-volumes of convex bodies
-ferromagnetic Ising
(Jerrum, Sinclair, Vigoda, Applegate, Kannan, Dyer, Frieze,...)

$$\text{i'th configuration } \Omega_i = b_i^1 \ldots b_i^n \text{ has probability } P(b_i^1 \ldots b_i^n)$$

$$\sum_i \sqrt{P(b_i^1 \ldots b_i^{n-1})}|b_i^1 \ldots b_i^{n-1}\rangle \left[\sqrt{P(b_i^n = 0|b_i^1 \ldots b_i^{n-1})}|0\rangle + \sqrt{P(b_i^n = 1|b_i^1 \ldots b_i^{n-1})}|1\rangle\right]$$

$$= \sum_i \sqrt{P(b_i^1 \ldots b_i^n)}|b_i^1 \ldots b_i^n\rangle$$

Q-SAMPLE

90's – Invasion of the Math Lords

Invasion I
Provably rapidly mixing
Markov chains

-permanents of +'ve matrices
-integrating log-concave functions
-volumes of convex bodies
-ferromagnetic Ising
(Jerrum, Sinclair, Vigoda, Applegate, Kannan, Dyer, Frieze,...)

$$\text{i'th configuration } \Omega_i = b_i^1 \ldots b_i^n \text{ has probability } P(b_i^1 \ldots b_i^n)$$

$$\sum_i \sqrt{P(b_i^1 \ldots b_i^{n-1})}|b_i^1 \ldots b_i^{n-1}\rangle \left[\sqrt{P(b_i^n = 0|b_i^1 \ldots b_i^{n-1})}|0\rangle + \sqrt{P(b_i^n = 1|b_i^1 \ldots b_i^{n-1})}|1\rangle\right]$$

$$= \sum_i \sqrt{P(b_i^1 \ldots b_i^n)}|b_i^1 \ldots b_i^n\rangle$$

Q-SAMPLE

Interesting?

$$\sum_j \sqrt{e^{-\beta E_j}}|j\rangle$$

90's – Invasion of the Math Lords

Invasion I

Provably rapidly mixing
Markov chains

-permanents of +'ve matrices
-integrating log-concave functions
-volumes of convex bodies
-ferromagnetic Ising
(Jerrum, Sinclair, Vigoda, Applegate, Kannan, Dyer, Frieze,...)

i'th configuration $\Omega_i = b_i^1 \ldots b_i^n$ has probability $P(b_i^1 \ldots b_i^n)$

$$\sum_i \sqrt{P(b_i^1 \ldots b_i^{n-1})}|b_i^1 \ldots b_i^{n-1}\rangle \left[\sqrt{P(b_i^n = 0|b_i^1 \ldots b_i^{n-1})}|0\rangle + \sqrt{P(b_i^n = 1|b_i^1 \ldots b_i^{n-1})}|1\rangle\right]$$

$$= \sum_i \sqrt{P(b_i^1 \ldots b_i^n)}|b_i^1 \ldots b_i^n\rangle$$

Q-SAMPLE

Interesting?

$$H^{\otimes n} \sum_j \sqrt{e^{-\beta E_j}}|j\rangle$$

90's – Invasion of the Math Lords

Invasion I
Provably rapidly mixing
Markov chains

-permanents of +'ve matrices
-integrating log-concave functions
-volumes of convex bodies
-ferromagnetic Ising
(Jerrum, Sinclair, Vigoda, Applegate, Kannan, Dyer, Frieze,...)

i'th configuration $\Omega_i = b_i^1 \ldots b_i^n$ has probability $P(b_i^1 \ldots b_i^n)$

$$\sum_i \sqrt{P(b_i^1 \ldots b_i^{n-1})}|b_i^1 \ldots b_i^{n-1}\rangle \left[\sqrt{P(b_i^n = 0|b_i^1 \ldots b_i^{n-1})}|0\rangle + \sqrt{P(b_i^n = 1|b_i^1 \ldots b_i^{n-1})}|1\rangle\right]$$

$$= \sum_i \sqrt{P(b_i^1 \ldots b_i^n)}|b_i^1 \ldots b_i^n\rangle$$

Q-SAMPLE

Interesting?

$$P(k) = \frac{1}{Z2^n}\left|\sum_j (-1)^{j\cdot k} e^{-\beta E_j/2}\right|^2$$

Coogee question 1: How crazy is this?

90’s – Invasion of the Math Lords

Invasion II

Exact sampling

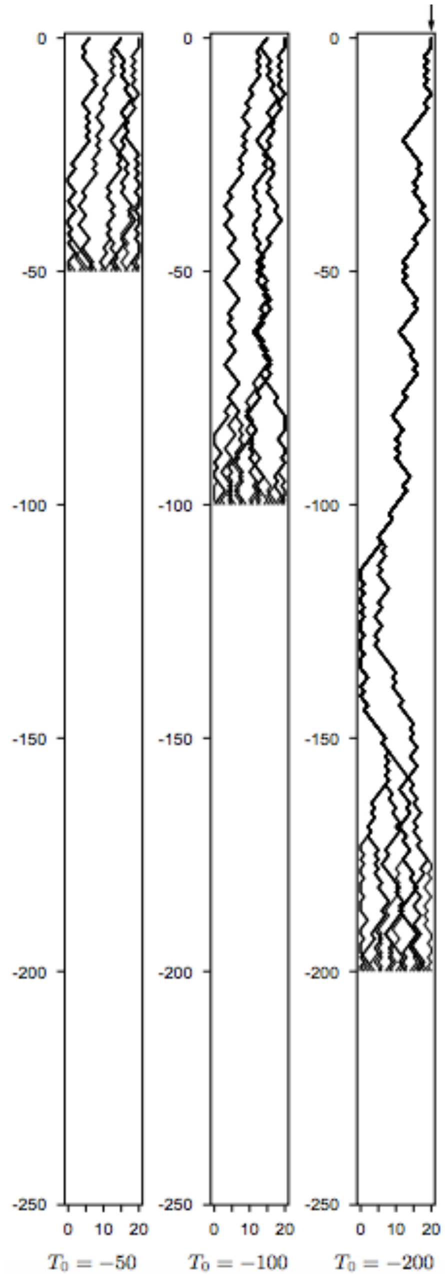
-”coupling from the past” (Propp, Wilson)

90’s – Invasion of the Math Lords

Invasion II

Exact sampling

-”coupling from the past” (Propp, Wilson)



From McKay, Information Theory

90's – Invasion of the Math Lords

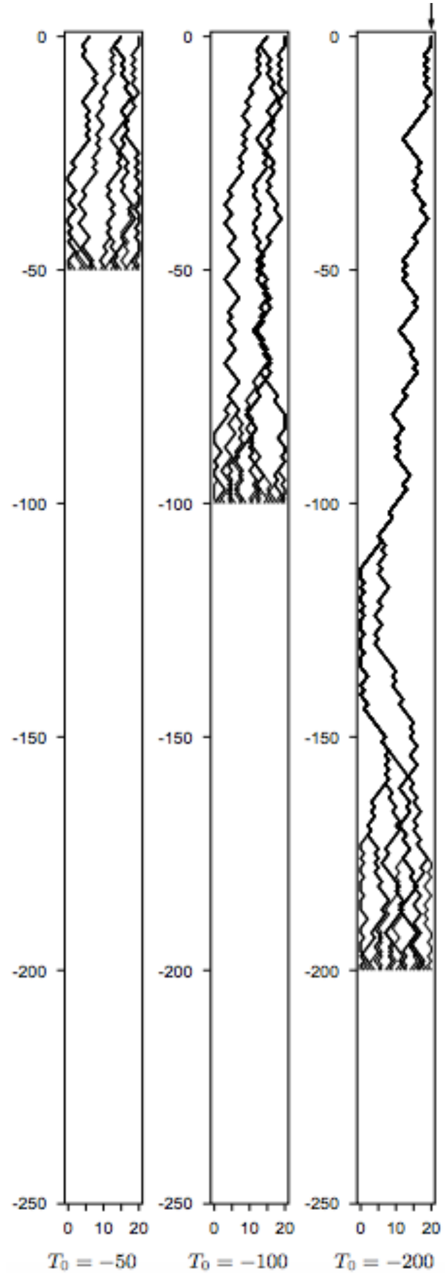
Invasion II

Exact sampling

-"coupling from the past" (Propp, Wilson)

Coogee question 2:

Can we "quantize" CFTP to make exact Q-samples?



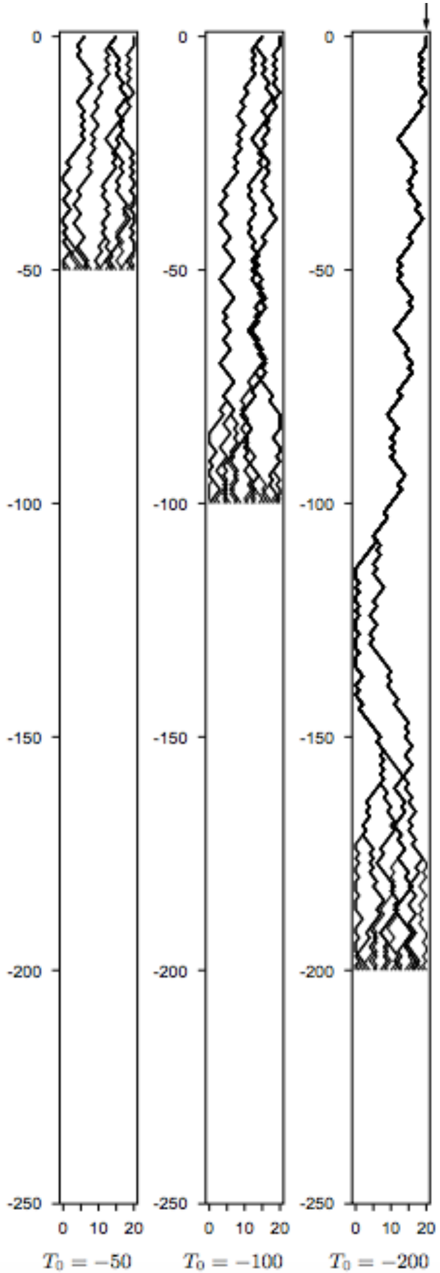
From McKay, Information Theory

90’s – Invasion of the Math Lords

Invasion II

Exact sampling

-”coupling from the past” (Propp, Wilson)



From McKay, Information Theory

Bernoulli Factory Problem:

Given the ability to exactly sample a distribution, what other distributions can also be exactly sampled by suitable processing?

90's – Invasion of the Math Lords

Invasion II

Exact sampling

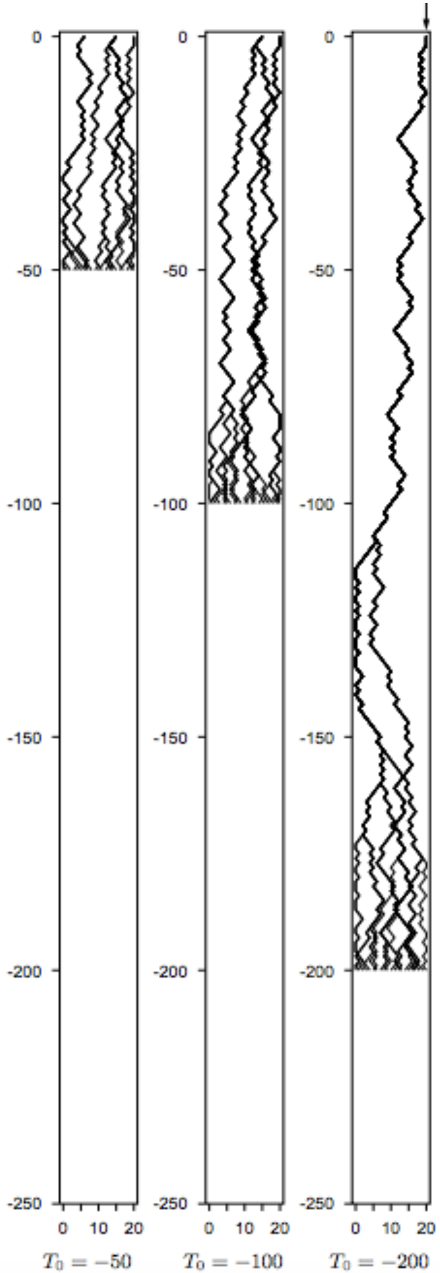
-"coupling from the past" (Propp, Wilson)

Bernoulli Factory Problem:

Given the ability to exactly sample a distribution, what other distributions can also be exactly sampled by suitable processing?

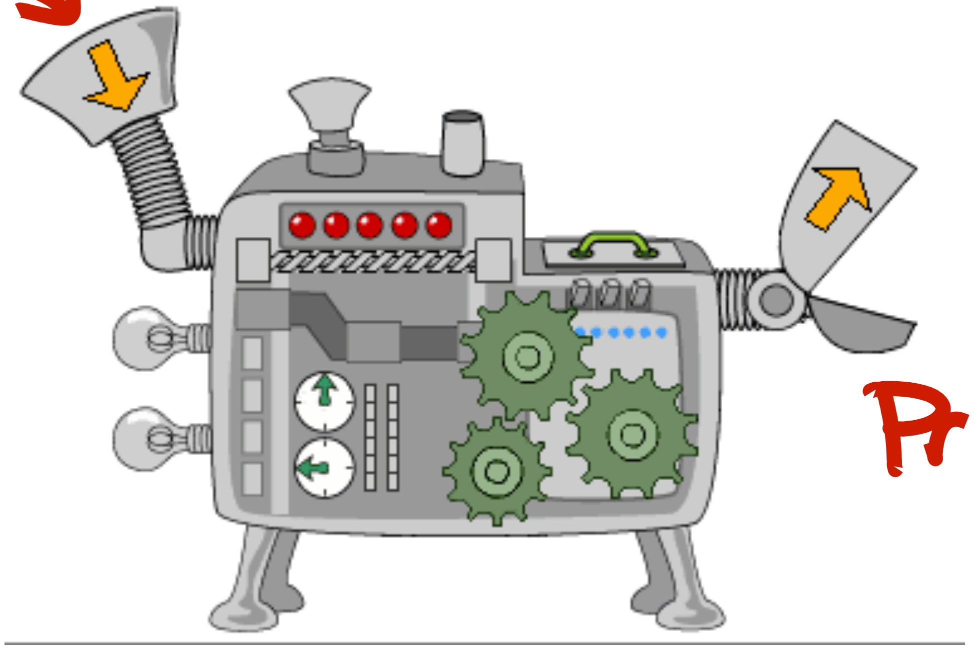
Most attention given to:

Given the ability to repeatedly sample a coin which is heads with probability *p*, for which functions *f* can we output a single new coin with probability of heads *f(p)*?



From McKay, Information Theory

$$\left.\begin{matrix}\vdots & \vdots & \vdots \\ T & H & T \\ H & T & T\end{matrix}\right\} \Pr(H) = p$$



H

$\Pr(H) = f(p)$

NOTE: unbounded input so not equivalent to Turing machine model

$$f(p) \quad = \quad p^2$$

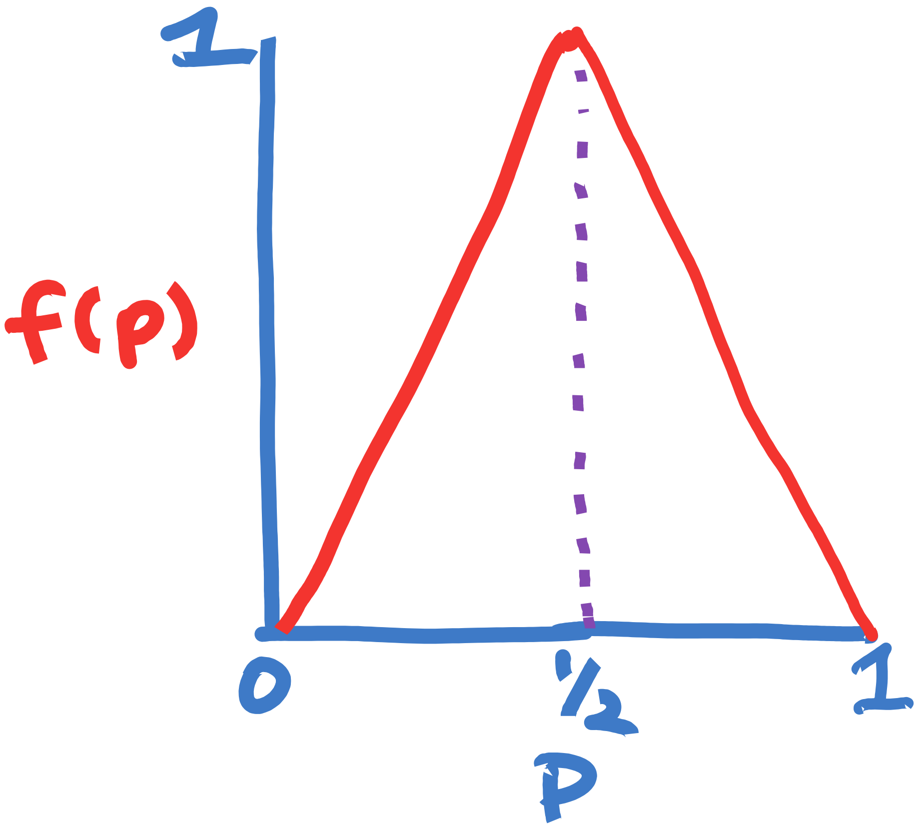
$$
\begin{aligned}
f(p) &= p^2 \\
f(p) &= 3p(1-p)
\end{aligned}
$$

$$
\begin{aligned}
f(p) &= p^2 \\
f(p) &= 3p(1-p) = 3p(1-p)^2 + 3p^2(1-p)
\end{aligned}
$$

$$
\begin{aligned}
f(p) &= p^2 \\
f(p) &= 3p(1-p) = 3p(1-p)^2 + 3p^2(1-p) \\
f(p) &= 1/2
\end{aligned}
$$

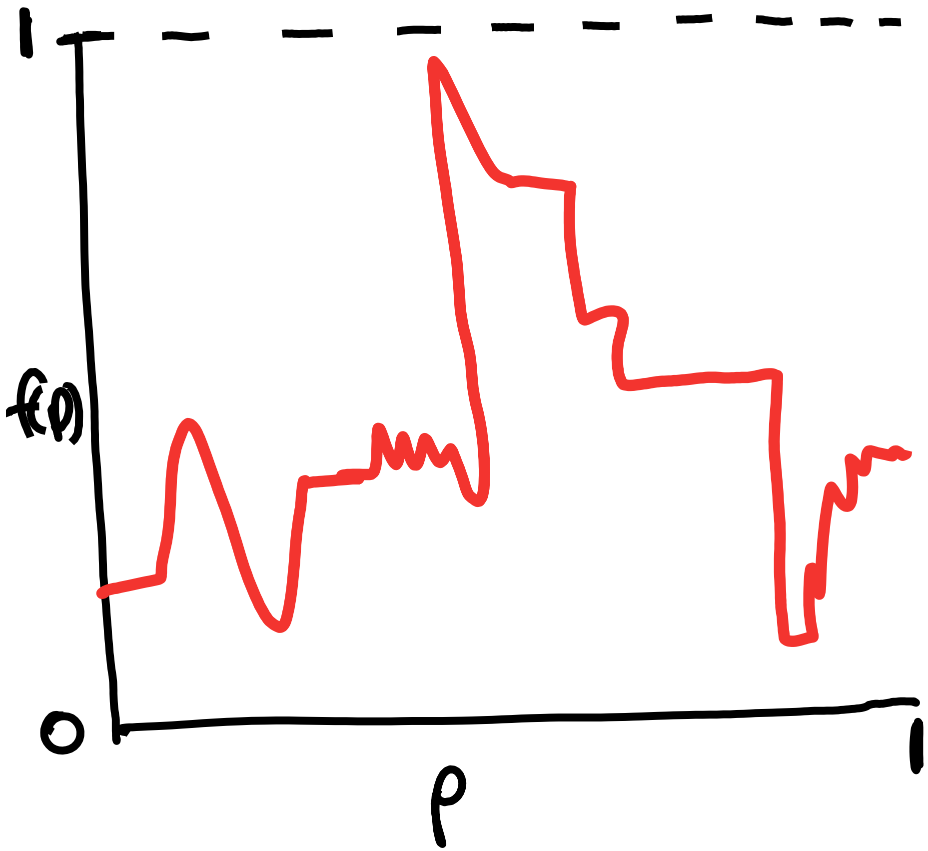
$$
\begin{aligned}
f(p) &= p^2 \\
f(p) &= 3p(1-p) = 3p(1-p)^2 + 3p^2(1-p) \\
f(p) &= 1/2 \\
f(p) &= \sqrt{p} = \sum_{k=1}^{\infty} \frac{\binom{2k}{k}}{2^{2k+1}(k+1)} (1-p)^{k+1}
\end{aligned}
$$

$$f(p) = \begin{cases} 2p & p \in (0, \tfrac{1}{2}] \\ 2(1-p) & p \in [\tfrac{1}{2}, 1) \end{cases}$$



"Probability Amplification"

GENERAL f(p)?



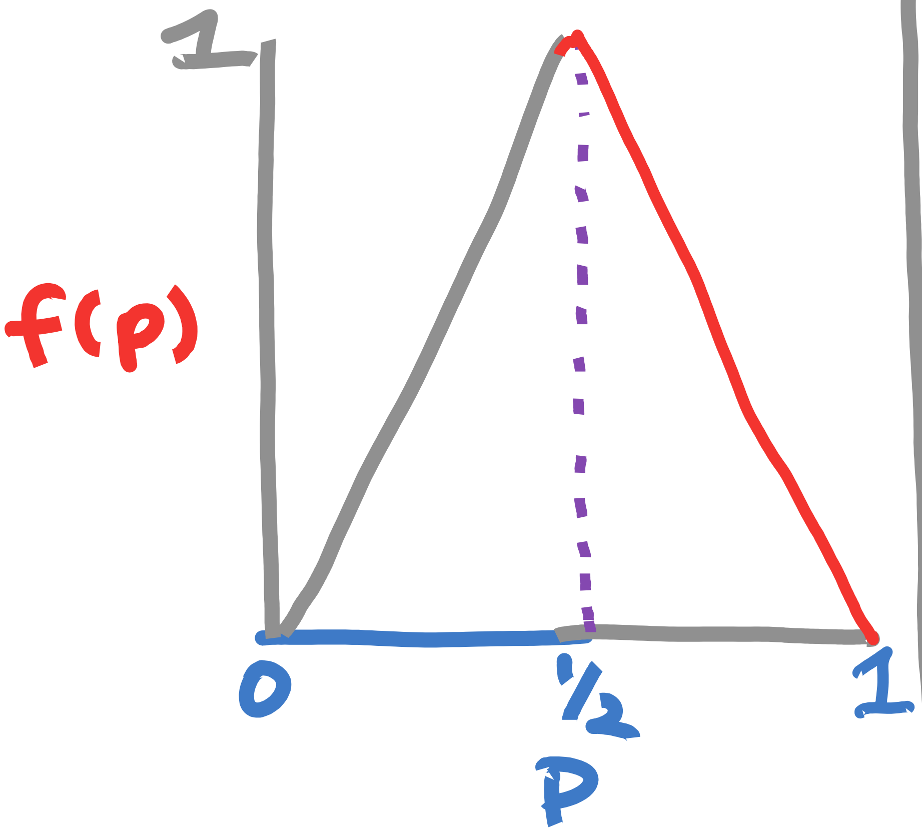
THEOREM

(Keane, O'Brien, '94)

$f(p)$ can be 'manufactured' iff f continuous & either f is constant, OR $\forall p, \exists k$ such that:

$$\min(f(p), 1-f(p)) \geq \min(p^k, (1-p)^k)$$

$$f(p) = 2p$$



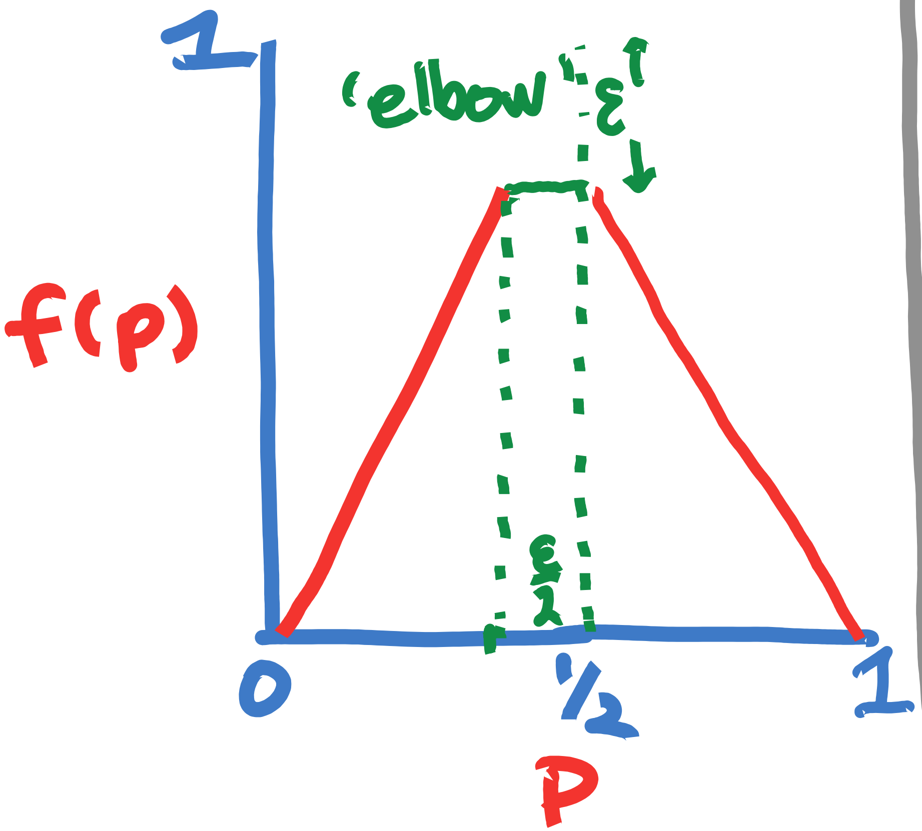
THEOREM

(Keane, O'Brien, '94)

$f(p)$ can be 'manufactured' iff f continuous & either f is constant, or $\forall p, \exists k$ such that:

$$\min(f(p), 1-f(p)) \geq \min(p^k, (1-p)^k)$$

$$f(p) = 2p$$



THEOREM

(Keane, O'Brien, '94)

$f(p)$ can be 'manufactured' iff f continuous & either f is constant, OR $\forall p, \exists k$ such that:

$$\min(f(p), 1-f(p)) \geq \min(p^k, (1-p)^k)$$

Simulating Events of Unknown Probabilities via Reverse Time Martingales

Krzysztof Łatuszyński
Department of Statistics
University of Warwick
Coventry, CV4 7AL

Ioannis Kosmidis
Department of Statistics
University of Warwick
Coventry, CV4 7AL

envelopes of f. To run the algorithm one has to construct sets of $\{0,1\}$ strings of appropriate cardinality based on coefficients of the polynomial envelopes. Unfortunately its naive implementation requires dealing with sets of exponential size (we encountered e.g. $2^{2^{26}}$) and thus is not very practical. Hence the authors

Electronic Journal of Statistics
Vol. 6 (2012) 10–37
ISSN: 1935-7524
DOI: 10.1214/11-EJS663

Exact sampling for intractable probability distributions via a Bernoulli factory

James M. Flegal

Department of Statistics
University of California, Riverside
e-mail: jflegal@ucr.edu

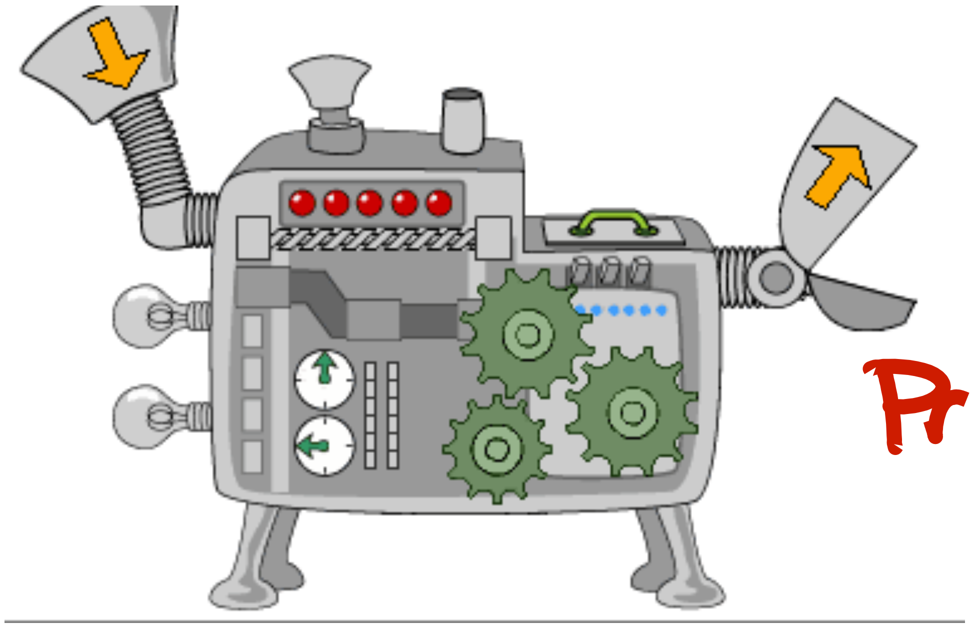
eration settings provided by Roy and Hobert (2007). This example is ill-suited using the proposed algorithm because of computational limitations related to the Bernoulli factory and in obtaining a practical ε. Specifically, we found (in simpler examples) obtaining a single draw from π sometimes required millions of i.i.d. τ variates. Unfortunately, even using non-constant $s(x)$, the probit example requires about 14,000 Markov chain draws per τ (Flegal and Jones, 2010). Hence obtaining a single draw from π would require an obscene number of draws from X. Implementation for more complicated Markov chains, such as this, likely requires further improvements, or a lot of patience.

COIN $p|0\rangle\langle 0| + (1-p)|1\rangle\langle 1|$

$$\Downarrow$$

QUOIN $\sqrt{p}\,|0\rangle + \sqrt{1-p}\,|1\rangle$

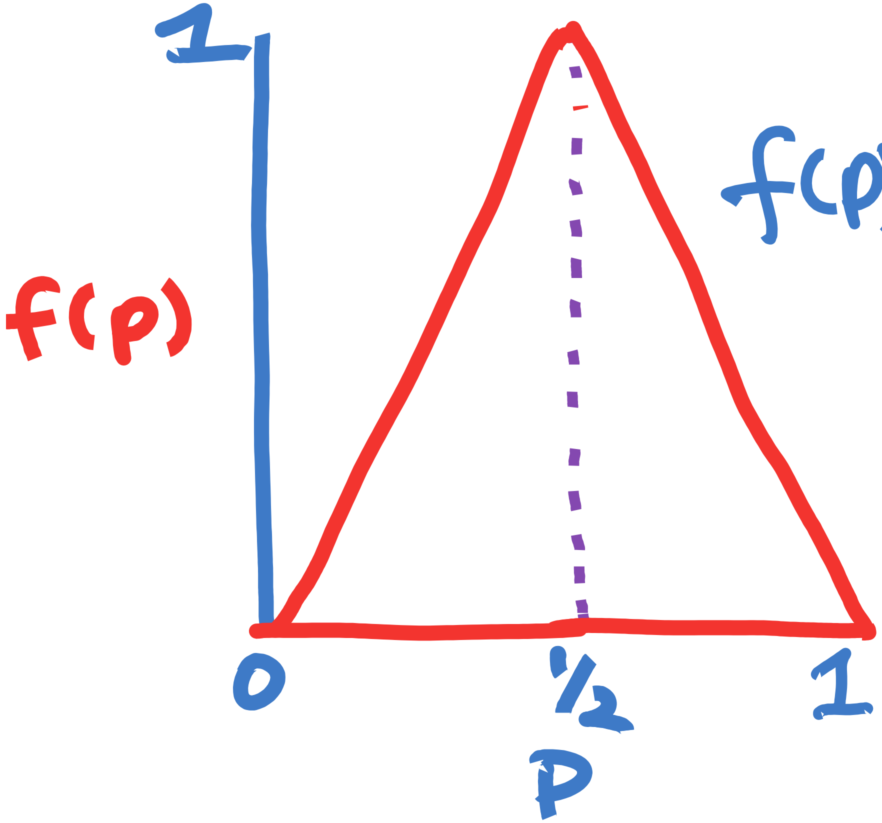
$$\sqrt{p}\,|0\rangle + \sqrt{1-p}\,|1\rangle$$



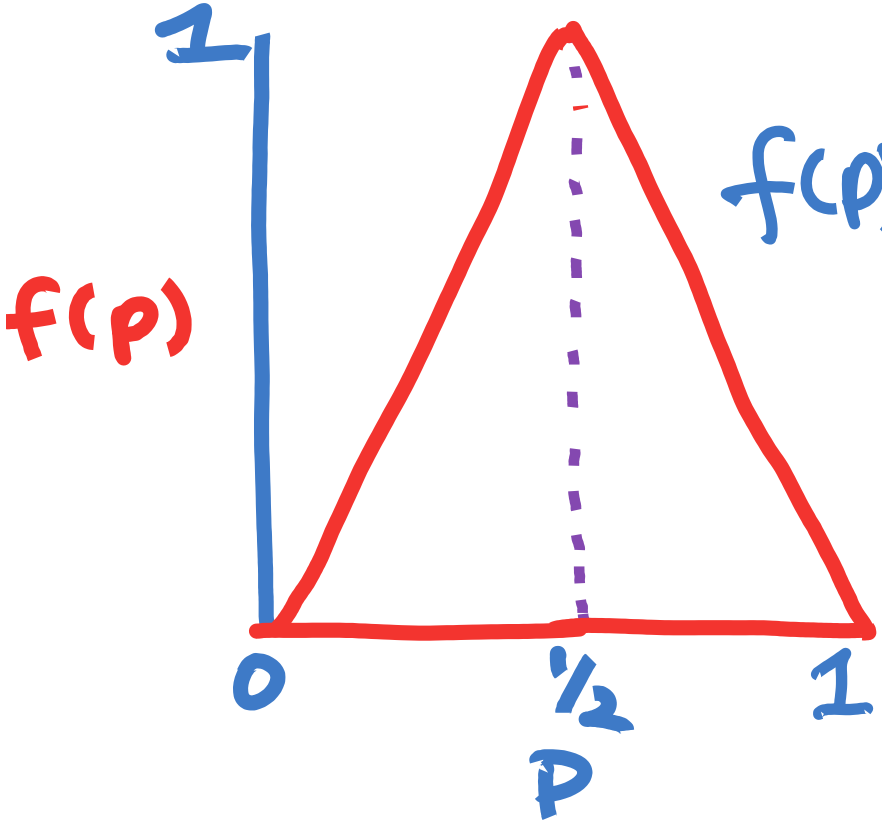
H

$$Pr(H) = f(p)$$

NOTE: unbounded input so not equivalent to Turing machine model

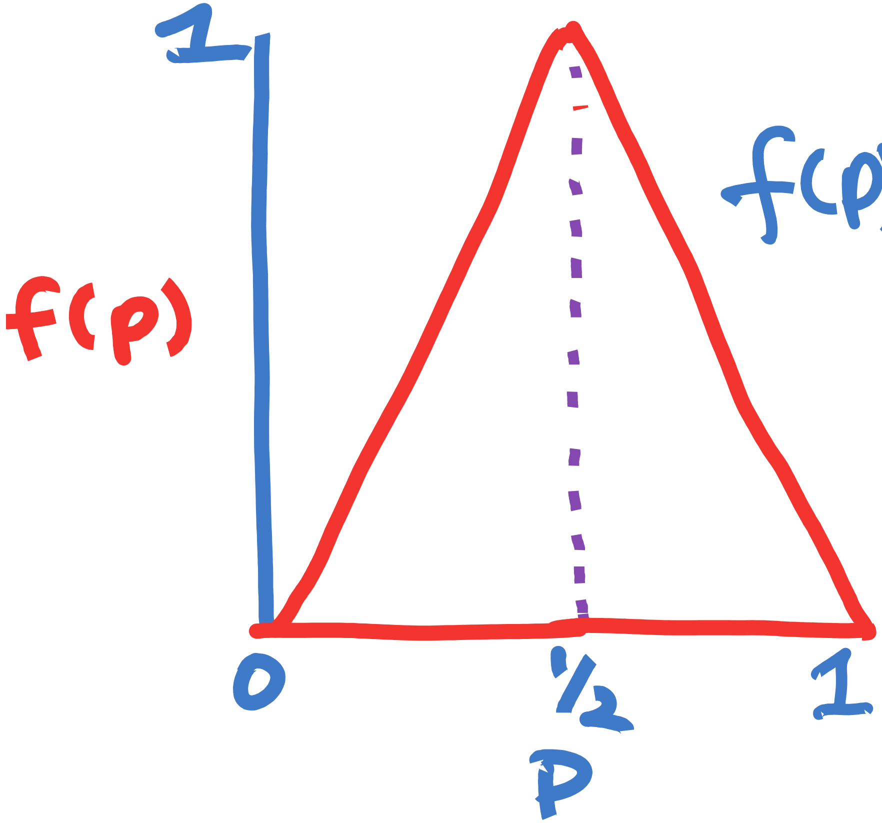


$$f(p) = 1 - \sqrt{1 - 4p(1-p)}$$



$$f(p) = 1 - \sqrt{1-4p(1-p)}$$

$$= \sum_{k=1}^{\infty} \binom{2k}{k} \frac{1}{(2k-1)4^k} \left[4p(1-p)\right]^k$$



$$f(p) = 1 - \sqrt{1 - 4p(1-p)}$$

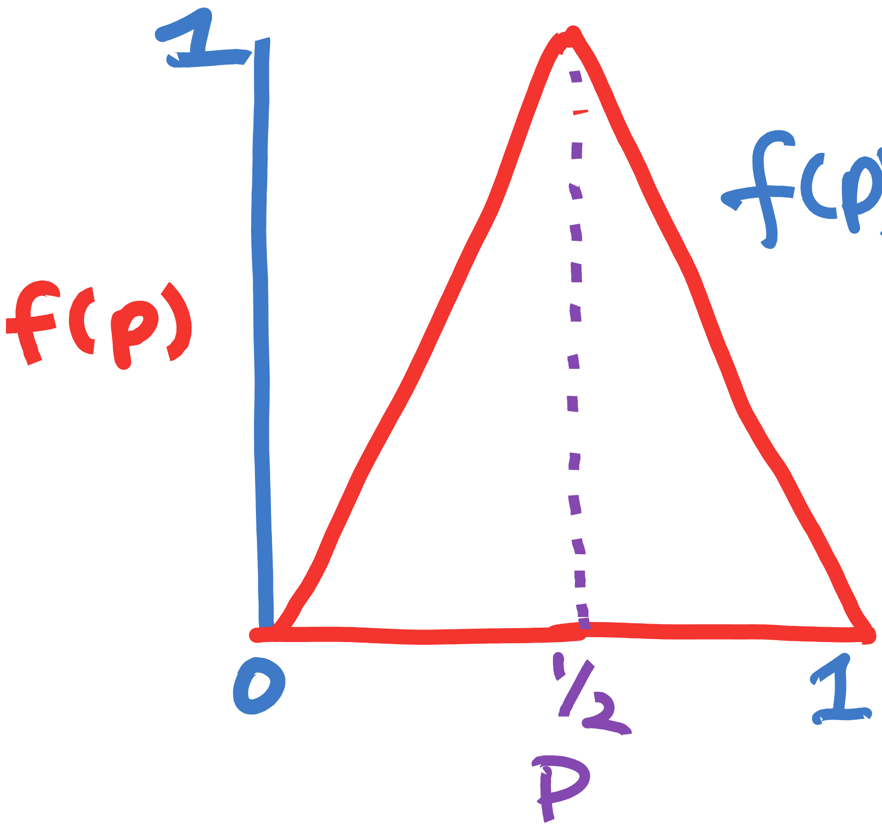
$$= \sum_{k=1}^{\infty} \binom{2k}{k} \frac{1}{(2k-1)4^k} [4p(1-p)]^k$$

$$\left(\sqrt{p}|0\rangle + \sqrt{1-p}|1\rangle\right)^{\otimes 2} = p|00\rangle + \sqrt{p}\sqrt{1-p}\sqrt{2}\,|\psi^+\rangle + (1-p)|11\rangle$$

$$Pr(|\phi^+\rangle) = \frac{1}{2}(p + (1-p))^2 = \frac{1}{2}$$

$$Pr(|\phi^-\rangle) = \frac{1}{2}(p - (1-p))^2 = \frac{1}{2}(2p-1)^2$$

$$Pr(|\psi^+\rangle) = 2p(1-p)$$



$$f(p) = 1 - \sqrt{1 - 4p(1-p)}$$

$$= \sum_{k=1}^{\infty} \binom{2k}{k} \frac{1}{(2k-1)4^k} [4p(1-p)]^k$$

$$\left(\sqrt{p}|0\rangle + \sqrt{1-p}|1\rangle\right)^{\otimes 2} = p|00\rangle + \sqrt{p}\sqrt{1-p}\sqrt{2}\,|\psi^+\rangle + (1-p)|11\rangle$$

$$\Pr(|\phi^+\rangle) = \frac{1}{2}(p + (1-p))^2 = \frac{1}{2}$$

$$\Pr(|\phi^-\rangle) = \frac{1}{2}(p - (1-p))^2 = \frac{1}{2}(2p-1)^2$$

$$\Pr(|\psi^+\rangle) = 2p(1-p)$$

$$\Pr(\psi^+ | \psi^+ \text{ or } \phi^+) = \frac{2p(1-p)}{1/2} = 4p(1-p)$$

FULL SET OF QUANTUM CONSTRUCTIBLE f(p)?

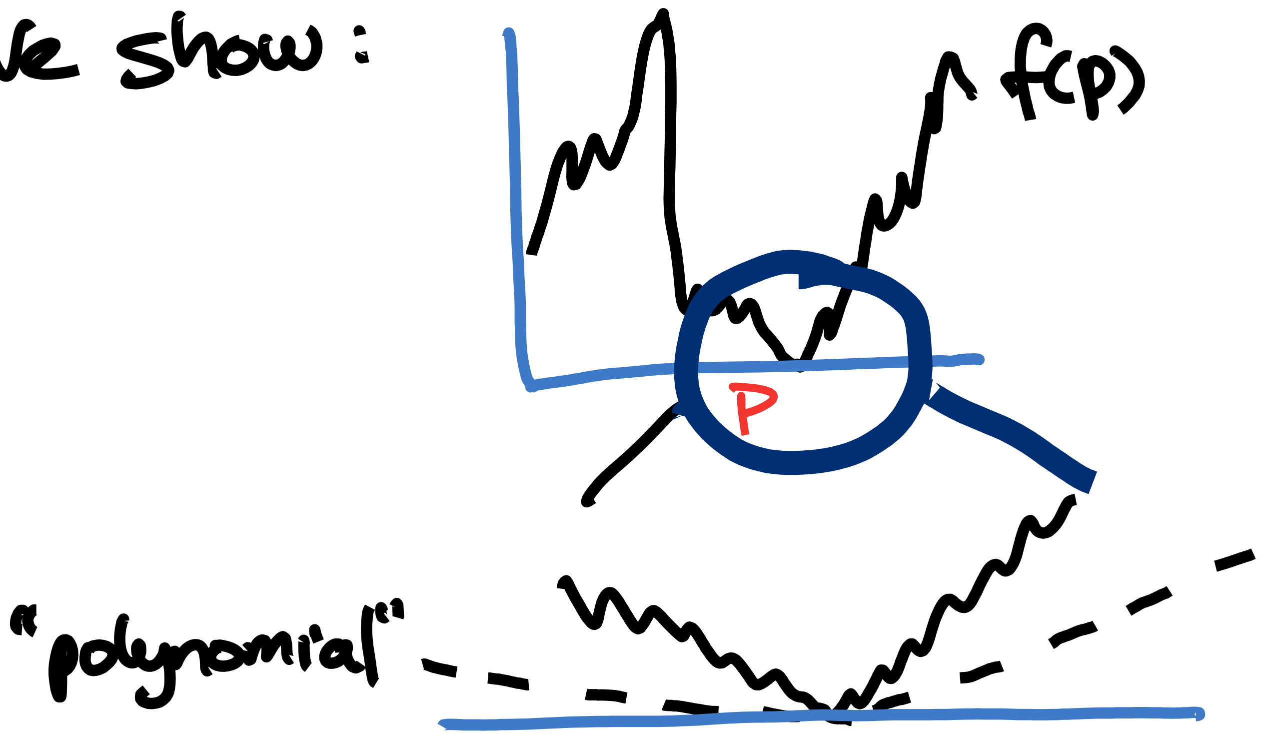
Theorem 1: a function f:[0, 1]→[0, 1] is constructible with quoins and a finite set of single-qubit operations if and only if the following conditions hold:

1. f is continuous.
2. Both $Z=\{z_i : f(z_i)=0\}$ and $W=\{w_i : f(w_i)=1\}$ are finite sets.
3. $\forall z \in Z$ there exists constants c, $\delta>0$ and and integer $k<\infty$ such that $c(p-z)^{2k} \le f(p) \forall p \in [z-\delta, z+\delta]$.
4. $\forall w \in W$ there exist constants c, $\delta>0$ and an integer $k<\infty$ such that $1-c(p-w)^{2k} \ge f(p) \forall p \in [w-\delta, w+\delta]$.

FULL SET OF QUANTUM CONSTRUCTIBLE f(p)?

constructible $\Leftrightarrow$ probability need to flip ∞ number of c/quoins is 0

We show:



Outline of the theorem proof:

Imagine we have constructible bounding functions:

$$L(p) \leq f(p) \leq U(p)$$

$$\max_{p \in [0,1]} (U(p) - L(p)) < \frac{1}{2}.$$

Outline of the theorem proof:

Imagine we have constructible bounding functions:

$$L(p) \le f(p) \le U(p)$$

$$\max_{p\in[0,1]} (U(p) - L(p)) < \frac{1}{2}.$$

Define sequence of constructible functions:

$$\begin{aligned}
f_1(p) &= f(p) \\
g_k(p) &= \frac{L_k(p)}{1 - U_k(p) + L_k(p)} \\
f_{k+1}(p) &= \frac{4}{3}\left(f_k(p) - \frac{1}{4} g_k(p)\right)
\end{aligned}$$

Outline of the theorem proof:

Imagine we have constructible bounding functions:

$$L(p) \leq f(p) \leq U(p)$$

$$\max_{p\in[0,1]} (U(p) - L(p)) < \frac{1}{2}.$$

Define sequence of constructible functions:

$$\begin{aligned} f_1(p) &= f(p) \\ g_k(p) &= \frac{L_k(p)}{1 - U_k(p) + L_k(p)} \\ f_{k+1}(p) &= \frac{4}{3}\left(f_k(p) - \frac{1}{4}g_k(p)\right) \end{aligned}$$

f(p) can be convexly decomposed:

$$f = \sum_{k=0}^{\infty} \left(\frac{3}{4}\right)^{k-1} \frac{1}{4} g_k(p).$$

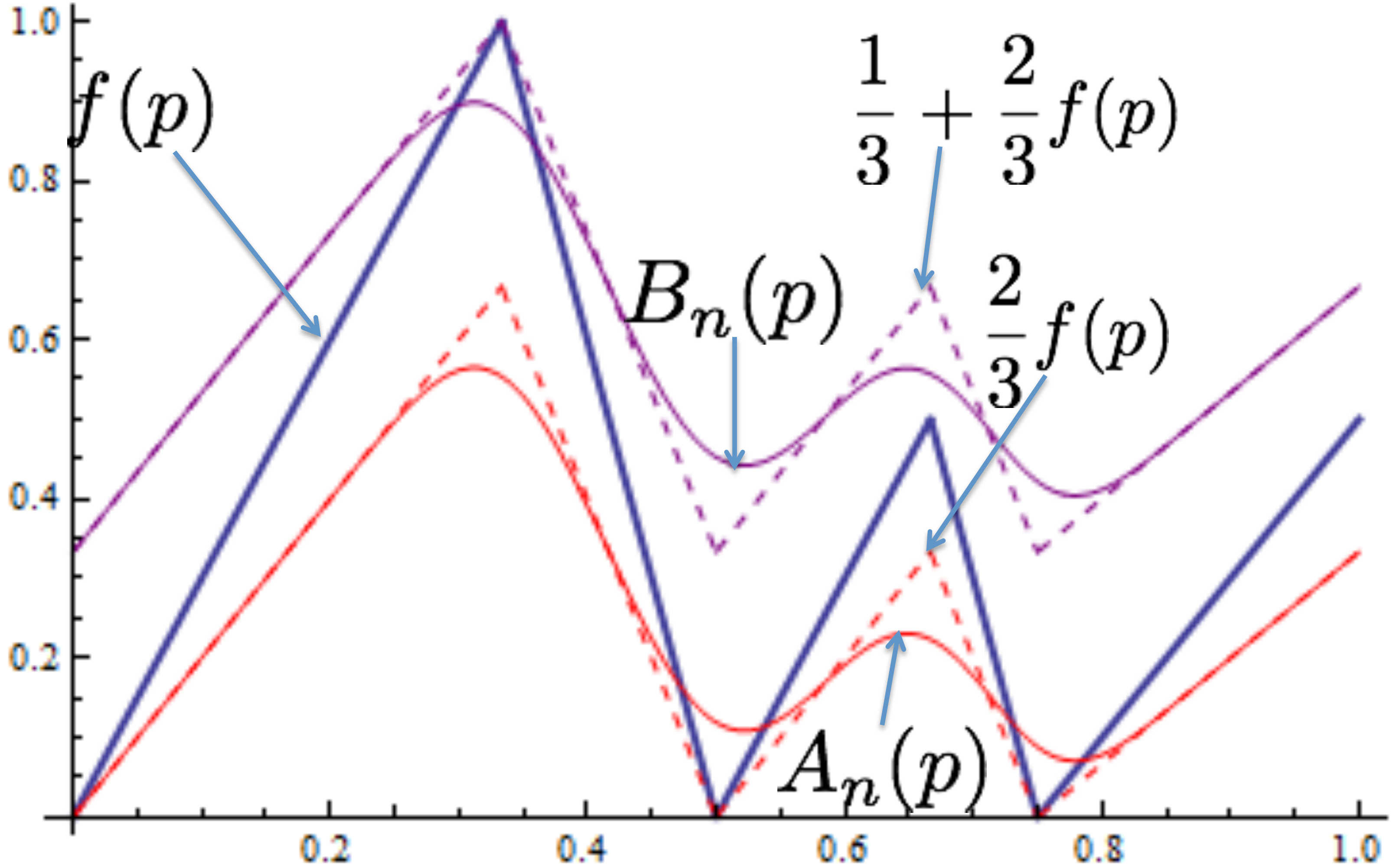
First guess for L(p) and U(p), Bernstein polynomial approximants:

$$
\begin{aligned}
A_n(p) &= \sum_{k=0}^{n} \frac{2}{3} f\left(\frac{k}{n}\right) \binom{n}{k} p^k (1-p)^{n-k} \\
B_n(p) &= \sum_{k=0}^{n} \left(\frac{1}{3} + \frac{2}{3} f\left(\frac{k}{n}\right)\right) \binom{n}{k} p^k (1-p)^{n-k}
\end{aligned}
$$

First guess for L(p) and U(p), Bernstein polynomial approximants:

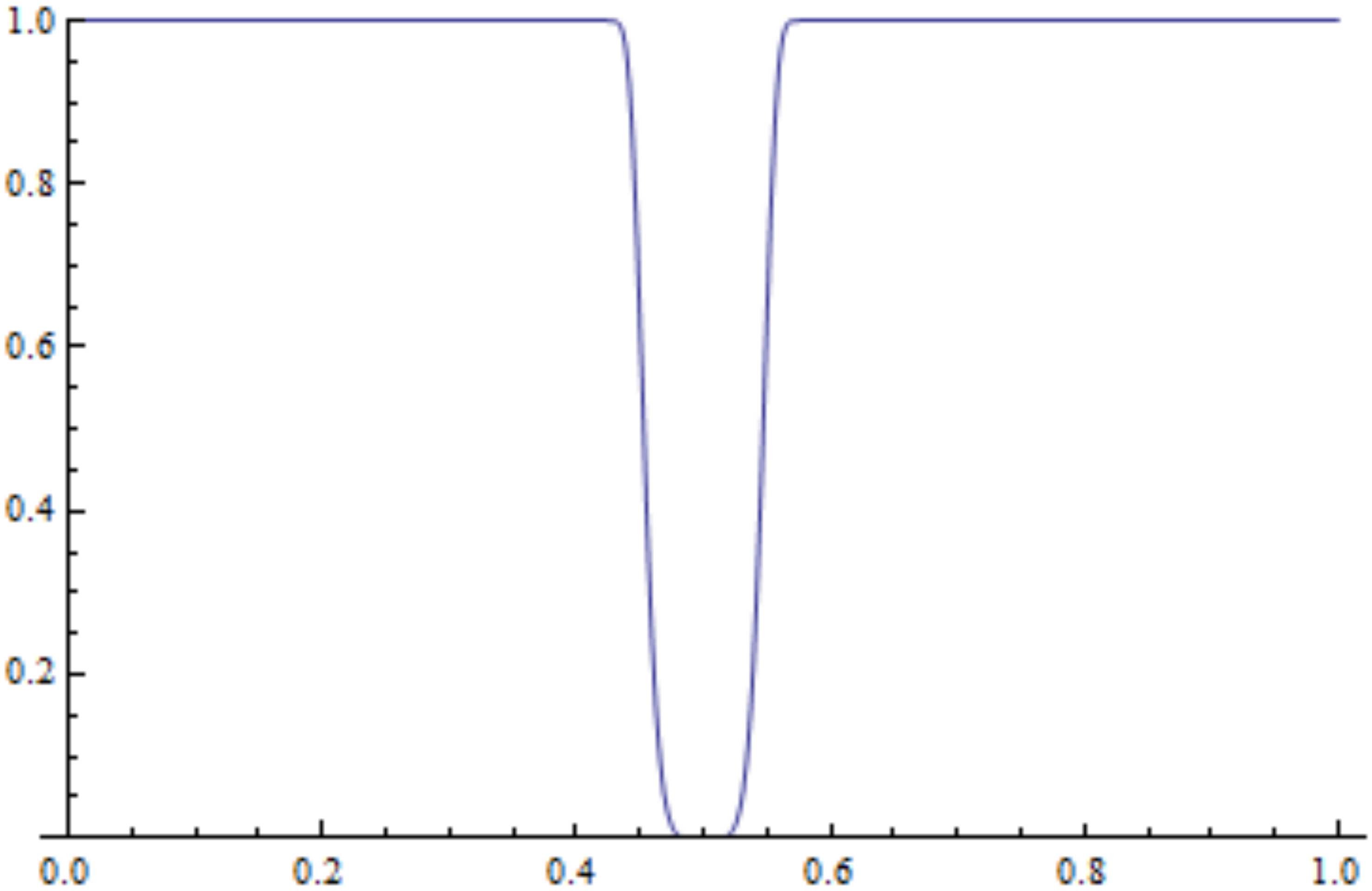
$$A_n(p) = \sum_{k=0}^{n} \frac{2}{3} f\left(\frac{k}{n}\right) \binom{n}{k} p^k (1-p)^{n-k}$$

$$B_n(p) = \sum_{k=0}^{n} \left(\frac{1}{3} + \frac{2}{3} f\left(\frac{k}{n}\right)\right) \binom{n}{k} p^k (1-p)^{n-k}$$

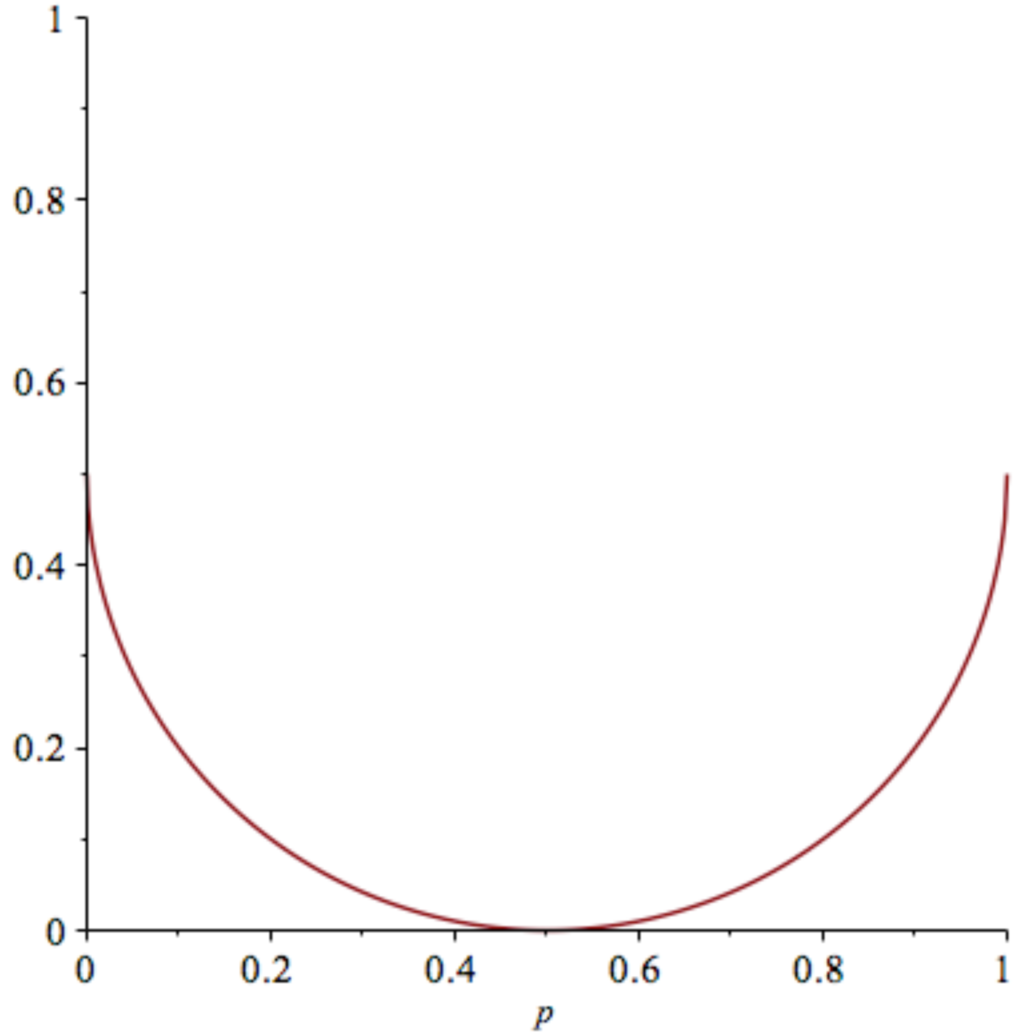


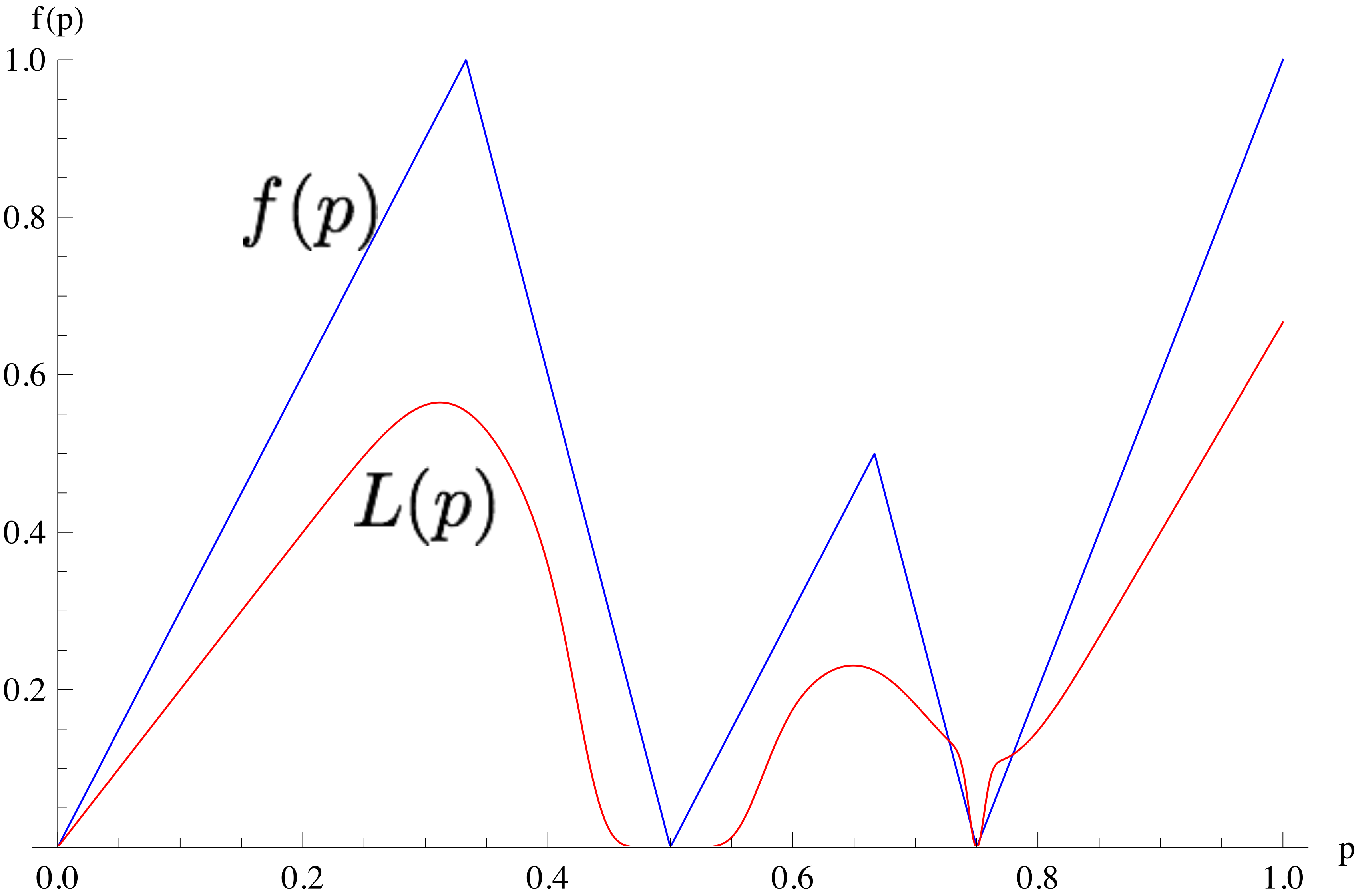
$$T_{m,M,z}(p) = (1 - (1 - h_z(p))^m))^M$$

$$h_z(p) = (\sqrt{1-z}\sqrt{p} - \sqrt{z}\sqrt{1-p})^2$$



$$h_z(p) = (\sqrt{1-z}\sqrt{p} - \sqrt{z}\sqrt{1-p})^2$$





f(p)
1.0
0.8
0.6
0.4
0.2
0.0
0.2
0.4
0.6
0.8
1.0
p
$f(p)$
$L(p)$

CONCLUSIONS

- Bernoulli factory mainly interesting because it leads to *provable* differences between classical info and quantum info

CONCLUSIONS

- Bernoulli factory mainly interesting because it leads to *provable* differences between classical info and quantum info

Coogee questions 4-6:

- Practical advantage?

- What the heck is the class of Q-sampleable distributions?

- For what set of functions *f(p)* can we implement:

$$\left(\sqrt{p}|0\rangle + \sqrt{1-p}|1\rangle\right)^{\otimes\infty} \longrightarrow \sqrt{f(p)}|0\rangle + \sqrt{1-f(p)}|1\rangle$$

"QUANTUM-QUANTUM-BERNOULLI FACTORY"