Title: Quoins versus Coins

Date: Mar 27, 2013 02:00 PM

URL: http://pirsa.org/13030000

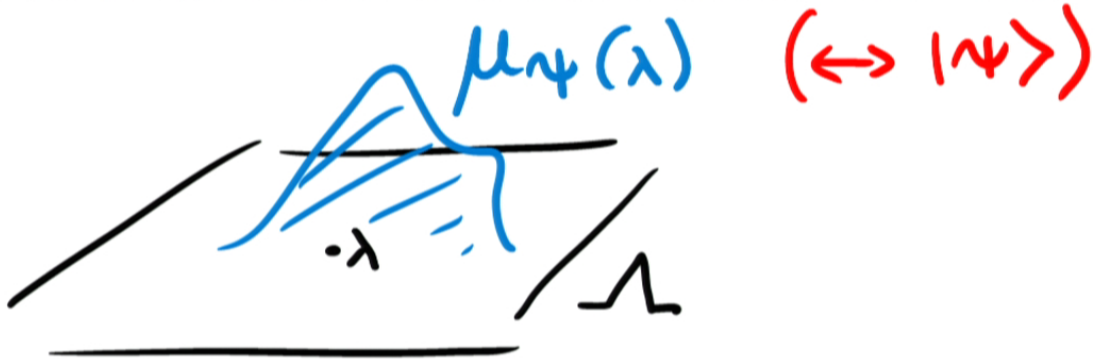
Abstract: Human monkeys are used to thinking about the problem of choosing from a set of objects according to some desired, biased, probability distribution. Just think about how you chose your partner(s). Even when it is easy for you to do such a sampling, it can be difficult to do a quantum sampling (Q-Sampling) of the same distribution. By Q-Sampling I mean the creation of a coherent superposition of states of such objects whose amplitudes are the (square roots of) of the specified distribution. In this talk I will discuss what we do know about this problem, why it is interesting, and will discuss how it can let us achieve tasks with quantum information that are provably impossible classically.

?

$$\rho = \sum_i p_i |i\rangle\langle i|$$

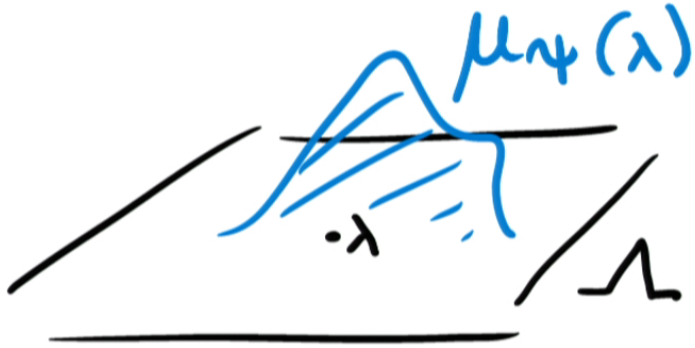
vs

$$|\psi\rangle = \sum_i \sqrt{p_i}\, |i\rangle$$



$(\leftrightarrow |\psi\rangle)$

$\text{size}(\lambda) \ll \text{size}(|\psi\rangle)$?



$(\leftrightarrow |\psi\rangle)$

$\text{size}(\lambda) \ll \text{size}(|\psi\rangle)$?

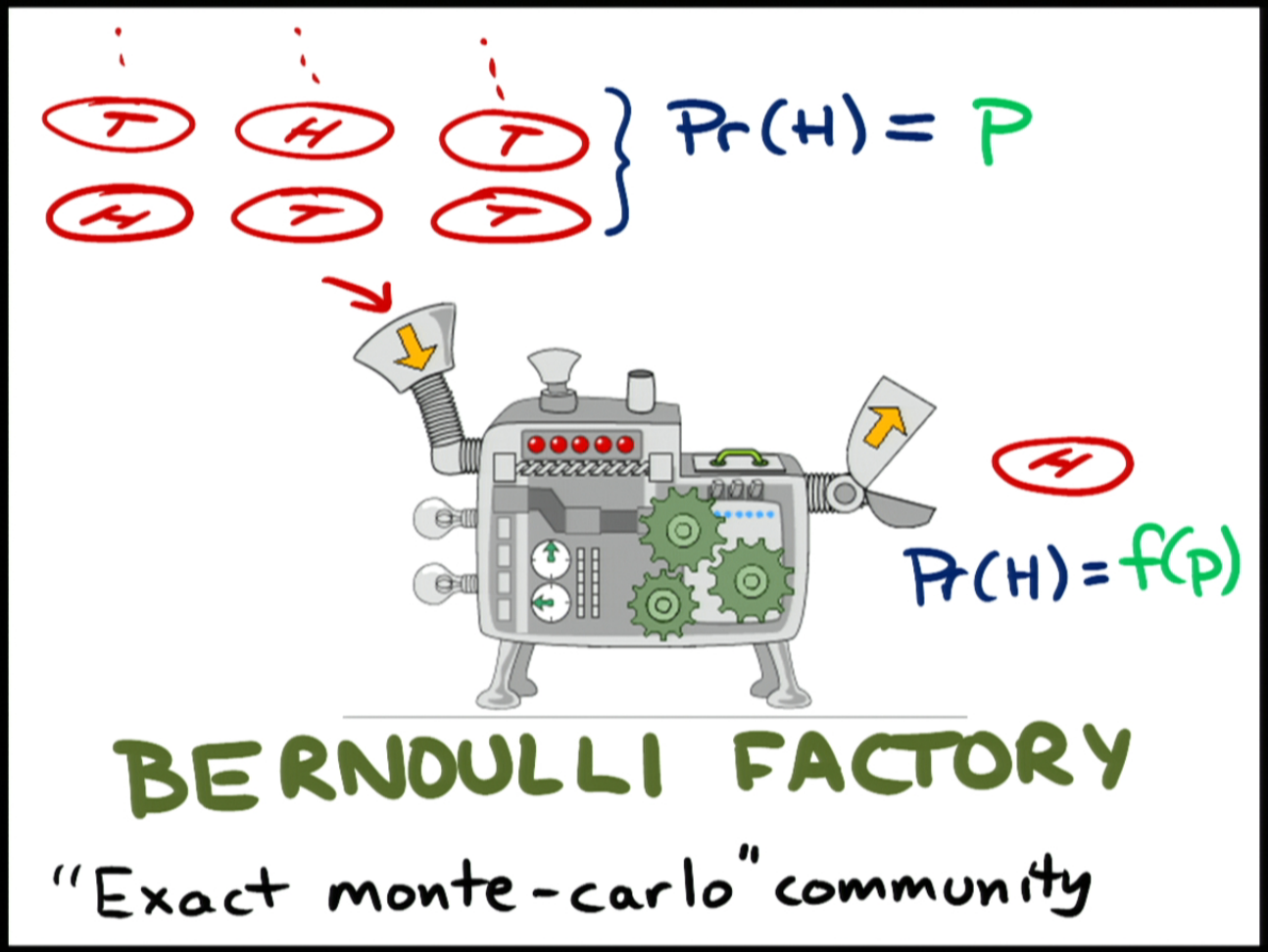
H T T H $\longrightarrow$ n bits

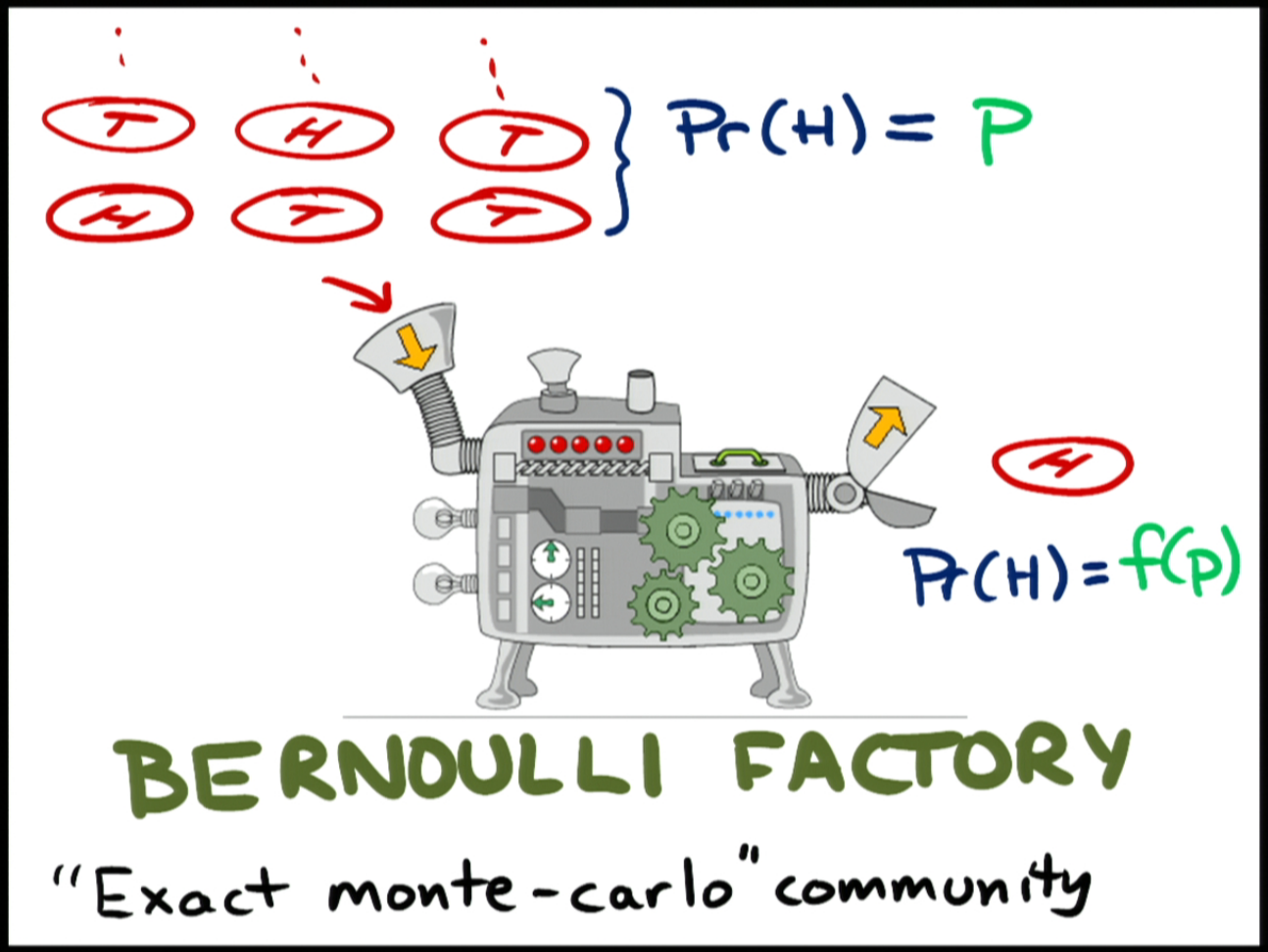
$\longrightarrow$ n bits

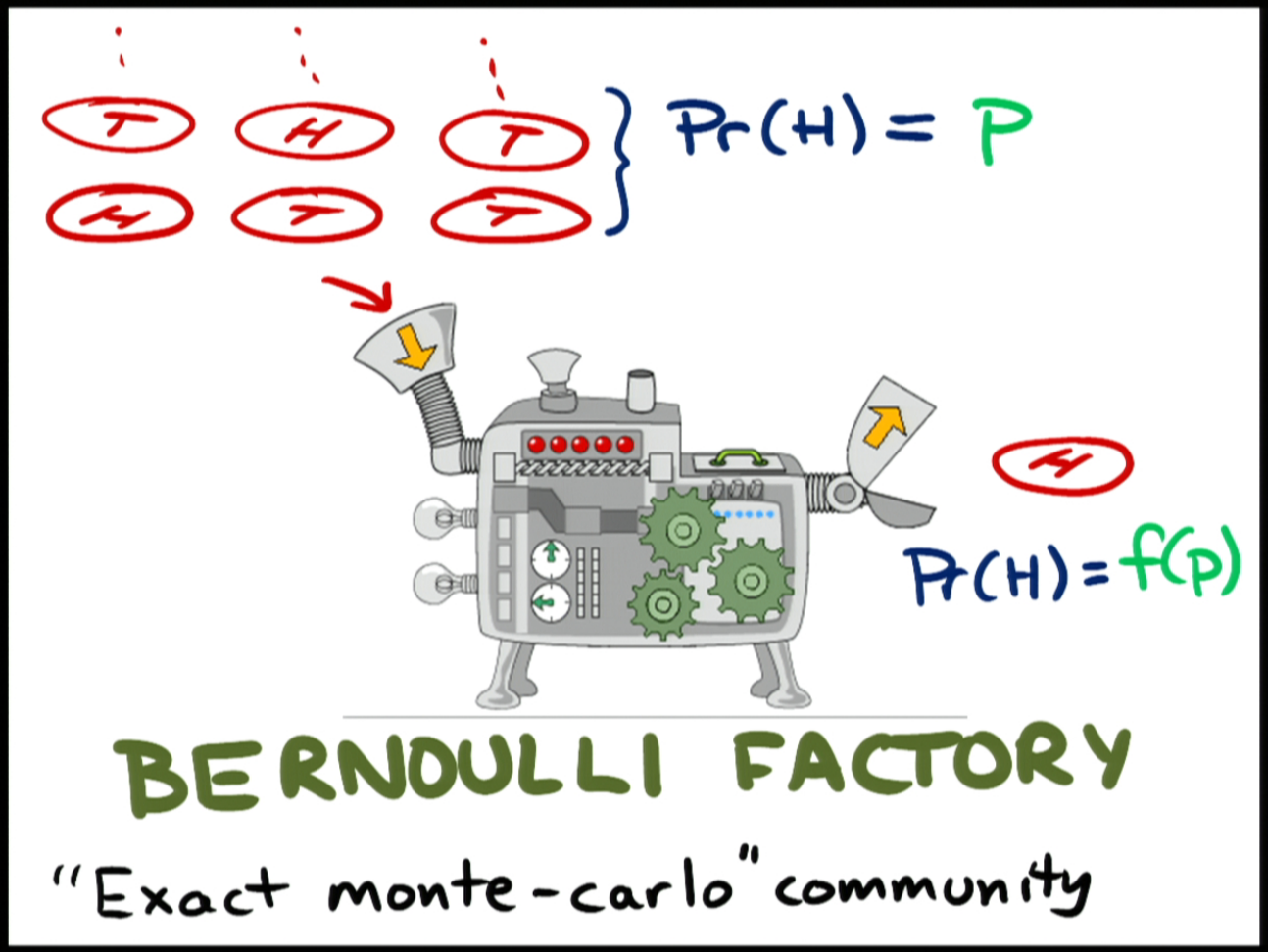
$\exists$ HVT such that

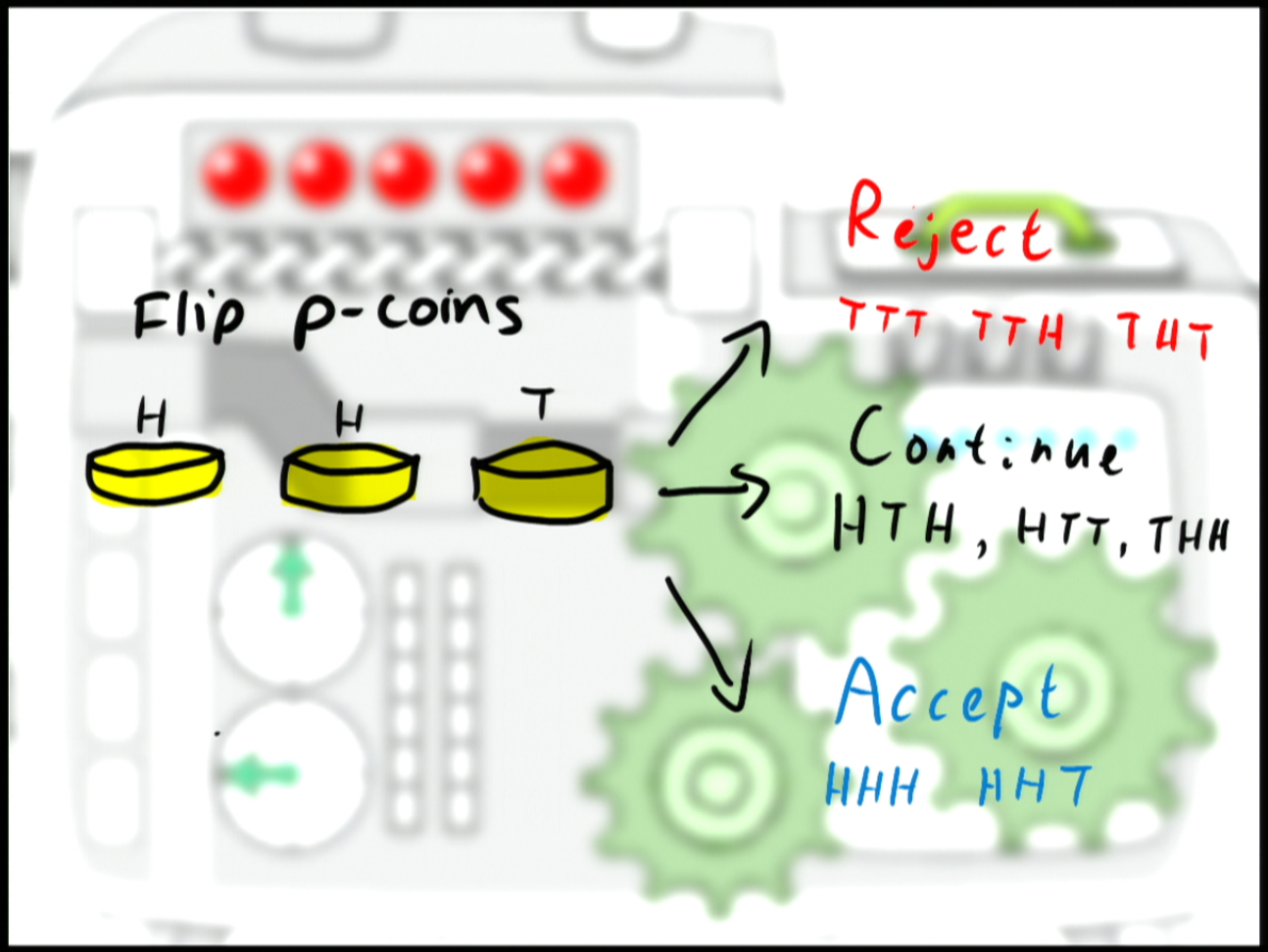
$\text{size}(\lambda) = O(n)$

$\Pr(\Pi \mid |\psi\rangle) = c_0 + c_1 \langle\psi|\Pi|\psi\rangle$


T H T
H T T
Pr(H) = p
Pr(H) = f(p)
BERNOULLI FACTORY
"Exact monte-carlo" community


T H T
H T T
Pr(H) = p
Pr(H) = f(p)
BERNOULLI FACTORY
"Exact monte-carlo" community


T H T
H T T
Pr(H) = P
Pr(H) = f(p)
BERNOULLI FACTORY
"Exact monte-carlo" community


Flip p-coins
H
H
T
Reject
TTT TTH THT
Continue
HTH, HTT, THH
Accept
HHH HHT

E.g. $$f(p) = \sum_{k=0}^{n} C_{nk}\, p^k (1-p)^{n-k}$$

integer $\leq \binom{n}{k}$

E.g. $$f(p) = \frac{p^2}{p^2 + (1-p)^2}$$

E.g. $$f(p) = \frac{p^2}{p^2 + (1-p)^2}$$

E.g. $f(p) = \frac{1}{2}$

E.g. $f(p) = \frac{1}{2}$

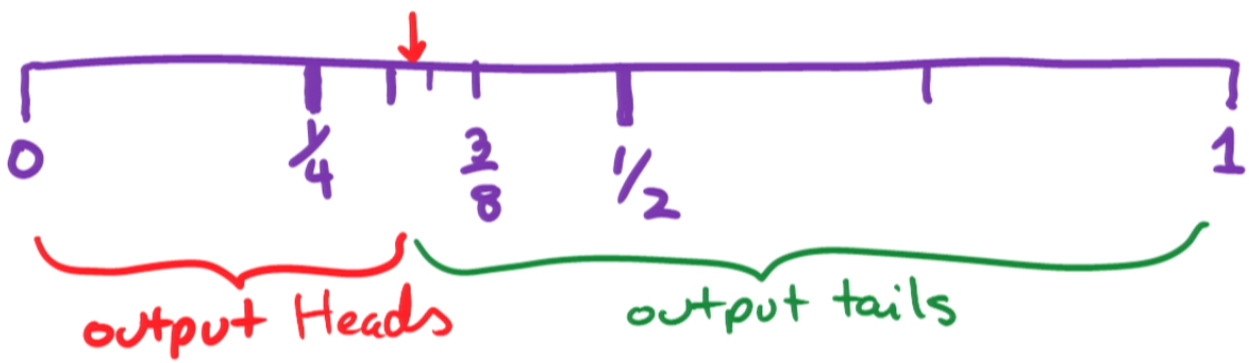
E.g. $f(p) = \frac{1}{2}$

k,n=2	$A_{2,k}$	$B_{4,k}$	$C_{2,k}$
0			00
1	10	01	
2			11

k,n=4	$A_{4,k}$	$B_{4,k}$	$C_{4,k}$
0			0000
1	0010,1000	0001,0100	
2	**0011**, 1010, 1001	0101, 0110, **1100**	
3	1110, 1011	1101, 0111	
4			1111

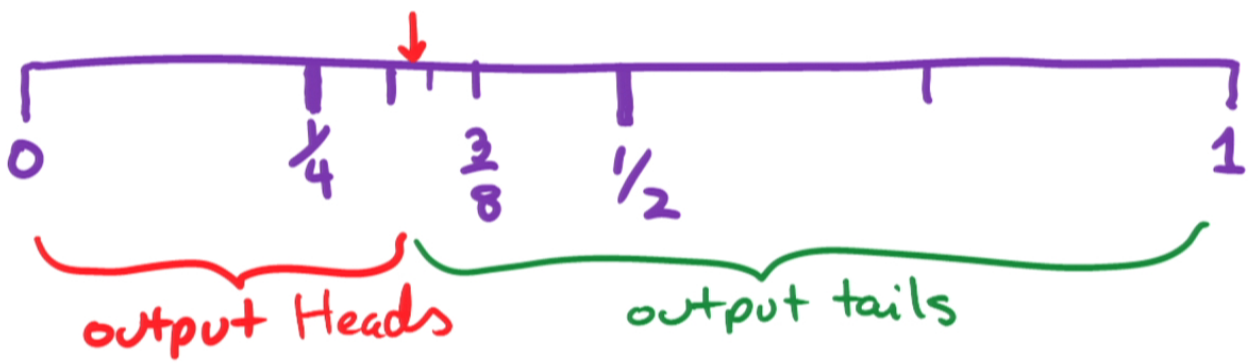
E.g. $f(p) = \frac{1}{\pi} = 0.318309\ldots$

$= 0.01010001011$

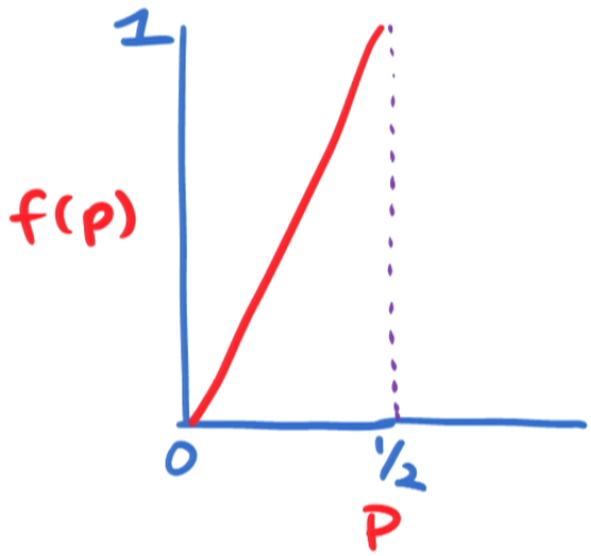


E.g. $f(p) = \frac{1}{\pi} = 0.318309\ldots$

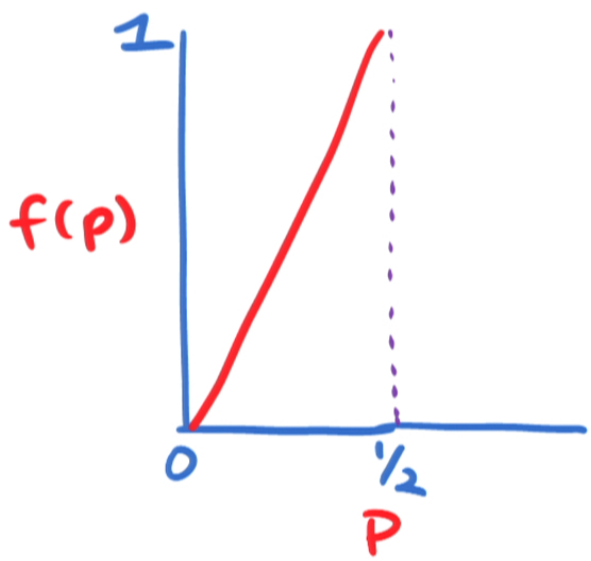
$=0.01010001011$



$$f(p) = 2p \qquad p \in (0, 1/2]$$



$$f(p) = 2p \qquad p \in (0, 1/2]$$



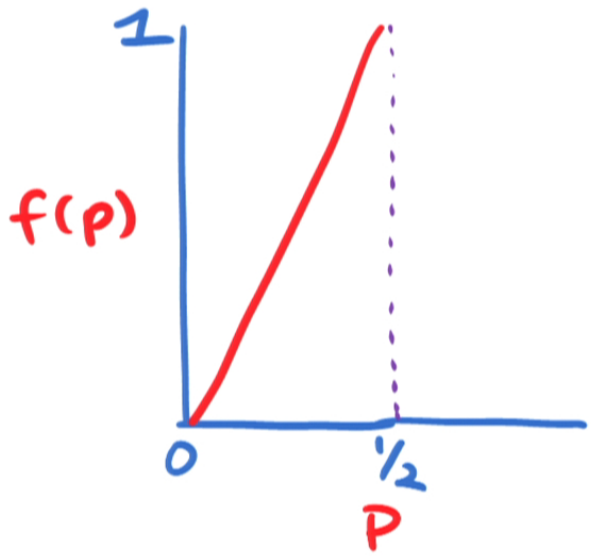
THEOREM

(Keane, O'Brien, '94)

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

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

$$f(p) = 2p \qquad p \in (0, 1/2]$$

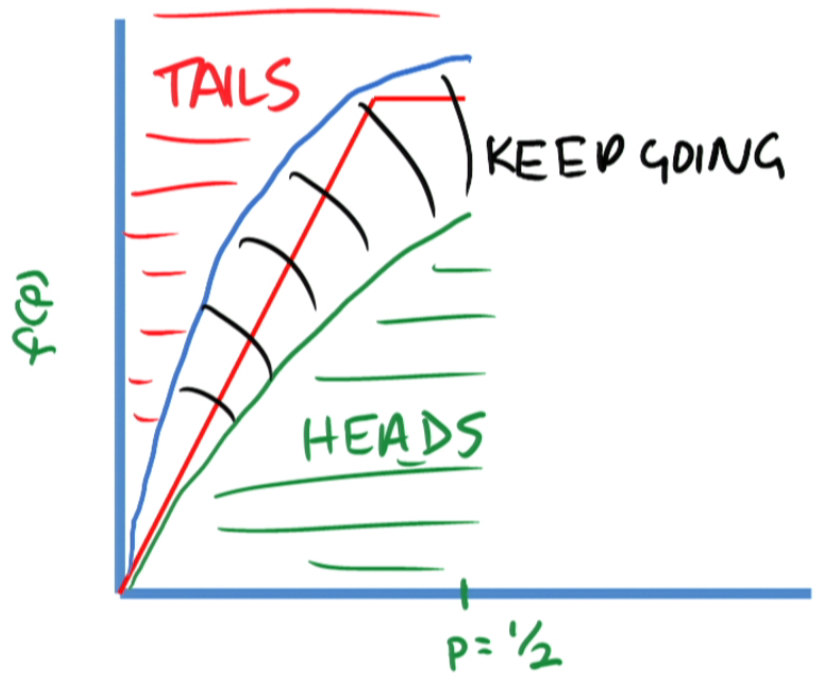


THEOREM

(Keane, O'Brien, '94)

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

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


TAILS
KEEP GOING
f(p)
HEADS
p = 1/2

INTRODUCING QUOINS:

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

$$\Downarrow$$

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

INTRODUCING QUOINS:

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

$$\Downarrow$$

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

Q-Sampling

$$\{p_i, \Omega_i\}$$

Ω_1 = Hugo = 01001
Ω_2 = David = 10110
Ω_3 = Mike = 01101

$$\sqrt{1/2}\,|01001\rangle + \sqrt{1/6}\,|10110\rangle + \sqrt{1/3}\,|01101\rangle \quad ?$$

Q-Sampling

$$\{p_i, \Omega_i\}$$

Ω_1 = Hugo = 01001
Ω_2 = David = 10110
Ω_3 = Mike = 01101

$$\sqrt{1/2}\,|01001\rangle + \sqrt{1/6}\,|10110\rangle + \sqrt{1/3}\,|01101\rangle \quad ?$$

E.G. PERMUTATIONS OF $1, 2, \ldots n$

$\Omega_1 = \sigma_1 = 123$

$\Omega_2 = \sigma_2 = 132$

$\vdots \quad \vdots \quad \vdots$

$$\underbrace{\left\{ P_i = \frac{1}{n!}, \Omega_i = \sigma_i \right\}}_{\text{Easy classically}}$$

ONE METHOD

- Choose $i \in \{1, \ldots, n!\}$ uniformly
- Compute σ_i

$$\frac{1}{\sqrt{n!}} \sum_i |i\rangle |\sigma_i\rangle \qquad \frac{1}{\sqrt{n!}} \sum_i |\sigma_i\rangle$$

E.G. PERMUTATIONS OF $1, 2, \ldots n$

$\Omega_1 = \sigma_1 = 123$

$\Omega_2 = \sigma_2 = 132$

$\vdots \qquad \vdots \qquad \vdots$

$$\underbrace{\left\{ P_i = \frac{1}{n!}, \Omega_i = \sigma_i \right\}}_{\text{Easy classically}}$$

ONE METHOD

- Choose $i \in \{1, \ldots, n!\}$ uniformly
- Compute σ_i

$$\cancel{\frac{1}{\sqrt{n!}} \sum_i |i\rangle |\sigma_i\rangle}$$

$$\boxed{\frac{1}{\sqrt{n!}} \sum_i |\sigma_i\rangle}$$

Q-SAMPLE

Q-SAMPLING & GRAPH ISOMORPHISM

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

$\sigma_0(G_1) = 101$

$\sigma_0(G_2) = 110$

Q-SAMPLING & GRAPH ISOMORPHISM

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

$\sigma_0(G_1) = 101$

$\sigma_1(G_1) = 101$

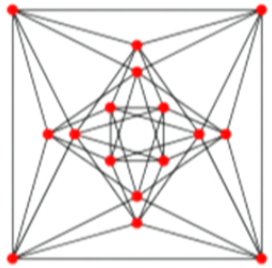
$\sigma_2(G_1) = 110$

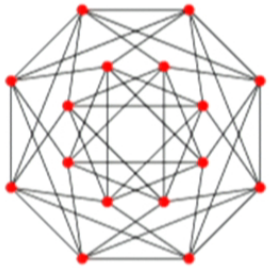
SAME

$\sigma_0(G_2) = 110$

$\sigma_1(G_2) = 011$

$\sigma_2(G_2) = 011$

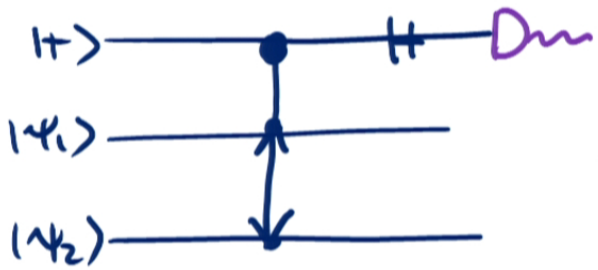




CLASSICAL (EASY) $\left\{ p_i = \frac{1}{n!} \, , \, \Omega_i = \sigma_i(G) \right\}$

POO SAMPLE (EASY) $\frac{1}{\sqrt{n!}} \sum_i |i\rangle |\sigma_i(G)\rangle$

SWAP TEST



$$|0\rangle|\psi_1\rangle|\psi_2\rangle + |1\rangle|\psi_2\rangle|\psi_1\rangle$$

$$P_{0/1} = \tfrac{1}{2}\left(1 \pm |\langle\psi_1|\psi_2\rangle|^2\right)$$

DOES NOT WORK FOR POO-SAMPLES

$$\left(\sum_i \langle i|\langle\sigma_i(G_1)|\right)\left(\sum_j |j\rangle|\sigma_j(G_2)\rangle\right)$$

$$= 0$$

Even if $G_1 = G_2$

WHAT CAN BE Q-SAMPLED?

ALL BIT STRINGS

$P_0 \ldots 00$ $\quad$ $0 \ldots 00$

$P_0 \ldots 01$ $\quad$ $0 \ldots 01$

$P_0 \ldots 10$ $\quad$ $0 \ldots 10$ $\quad$ P_1, Ω_1

$\vdots$ $\quad$ $\vdots$

WHAT CAN BE Q-SAMPLED?

RECENTLY DISCOVERED POWERFUL CLASSES OF CLASSICAL SAMPLING ALGORITHMS SOLVING HARD PROBLEMS:

- Ferromagnetic Ising (Jerrum, Sinclair)
- Permanents of non-negative matrices (Jerrum, Sinclair and Vigoda)
- Volumes of convex bodies in high dimensions (Dyer, Frieze, Kannan)
- Integration of log-concave functions (Applegate, Kannan)

"Self Reducible"

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

Quantum Physics

Creating superpositions that correspond to efficiently integrable probability distributions

Lov Grover, Terry Rudolph

WHAT CAN BE Q-SAMPLED?

$n=2$ example

$$\sqrt{P_{00}+P_{01}}\,|0\rangle + \sqrt{P_{10}+P_{11}}\,|1\rangle$$

$$\sqrt{P_{00}}\,|00\rangle + \sqrt{P_{01}}\,|01\rangle + \sqrt{P_{10}}\,|10\rangle + \sqrt{P_{11}}\,|11\rangle$$

WHAT CAN BE Q-SAMPLED?

$\boxed{\begin{array}{c} n=2 \\ \text{example} \end{array}}$

$$\sqrt{P_{00}+P_{01}}\,|0\rangle + \sqrt{P_{10}+P_{11}}\,|1\rangle$$

$$\rightarrow \sqrt{P_{00}+P_{01}}\,|0\rangle\left|\frac{P_{00}}{P_{00}+P_{01}}\right\rangle + \sqrt{P_{10}+P_{11}}\,|1\rangle\left|\frac{P_{10}}{P_{10}+P_{11}}\right\rangle$$

$$\sqrt{P_{00}}\,|00\rangle + \sqrt{P_{01}}\,|01\rangle + \sqrt{P_{10}}\,|10\rangle + \sqrt{P_{11}}\,|11\rangle$$

WHAT CAN BE Q-SAMPLED?

arXiv.org > quant-ph > arXiv:quant-ph/0301023

Quantum Physics

Adiabatic Quantum State Generation and Statistical Zero Knowledge

Dorit Aharonov, Amnon Ta-Shma

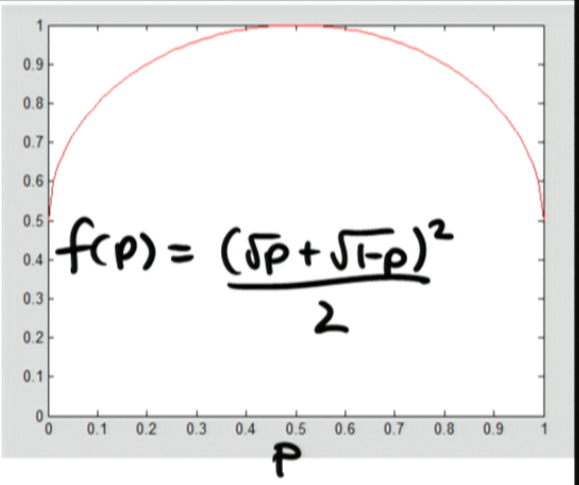
- (Only?) Results potentially applicable to non-self-reducible problems.

THEOREM

(Keane, O'Brien, '94)

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

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

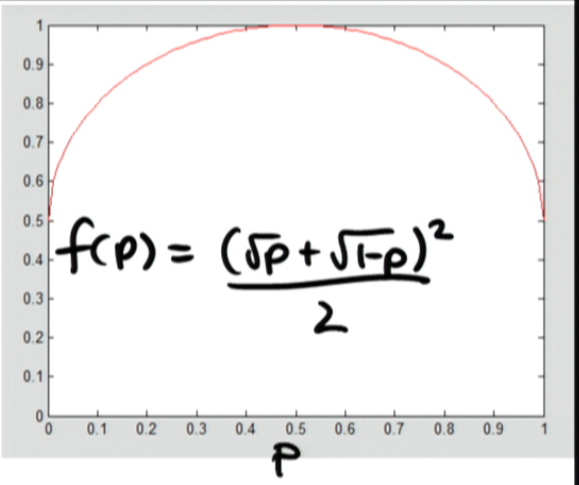


THEOREM

(Keane, O'Brien, '94)

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

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



$$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}\sqrt{p}\\ \sqrt{1-p}\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}\sqrt{p}+\sqrt{1-p}\\ \sqrt{p}-\sqrt{1-p}\end{bmatrix}$$

QUOINS INFINTELY MORE POWERFUL THAN CANS!!

MUCH MORE FUN TO BE HAD

- What functions can Quoins sample?

MUCH MORE FUN TO BE HAD

- What functions can Quoins sample?
- Quoinage savings for $f = 2p$?
- Joint measurements more powerful?
- Doubly-Quantum Bernouill factory?

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

SOME LAST FUN WITH Q-SAMPLING

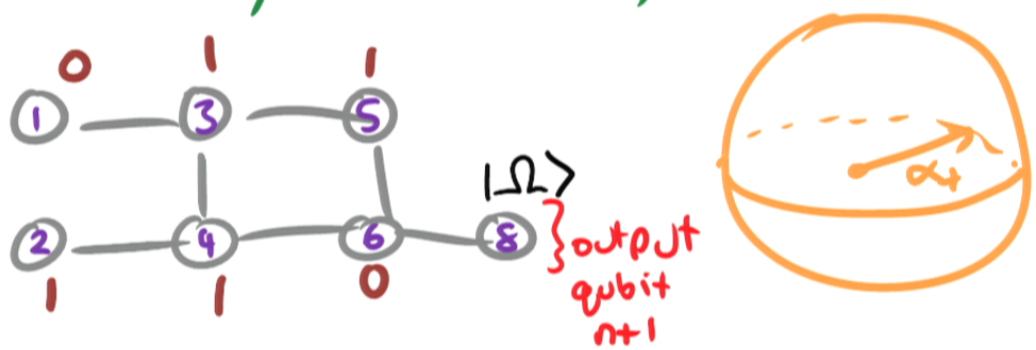
- Why does computation take time?

  circuits, adiabatic, cluster...

SOME LAST FUN WITH Q-SAMPLING

- Why does computation take time?

  circuits, adiabatic, cluster...



- Q-Sample all measurement records that output $|\Omega\rangle$ [NOT $X|\Omega\rangle$, $Z|\Omega\rangle$ etc]

$$|\mu\rangle = |000\cdots0\rangle + \cdots |001101\cdots\rangle + \cdots \quad O(2^n) \text{ terms}$$

$$|\mu\rangle \Rightarrow \cdots + \cdots |\alpha_+ \beta_+ \gamma_- \delta_- \cdots\rangle + \cdots$$

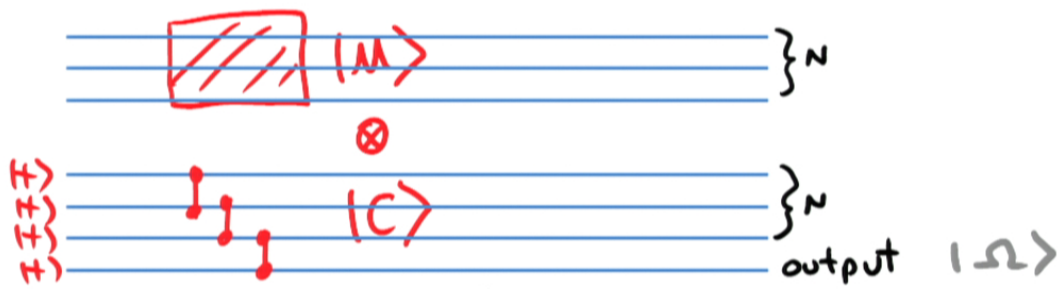
$$\left(\Pi_i = |\phi_i\rangle\langle\phi_i|, \ \sum_i |\phi_i\rangle\right)$$

- Q-Sample all measurement records that output $|\Omega\rangle$ [NOT $X|\Omega\rangle$, $Z|\Omega\rangle$ etc]

$$|M\rangle = |000\cdots0\rangle + \cdots |001101\cdots\rangle + \cdots \quad O(2^n) \text{ terms}$$

$$|M\rangle \Rightarrow \cdots + \cdots |\alpha_+ \beta_+ \cdots \gamma_- \delta_- \cdots\rangle + \cdots$$

$$\left(\Pi_i = |\phi_i\rangle\langle\phi_i|, \ \sum_i |\phi_i\rangle\right)$$

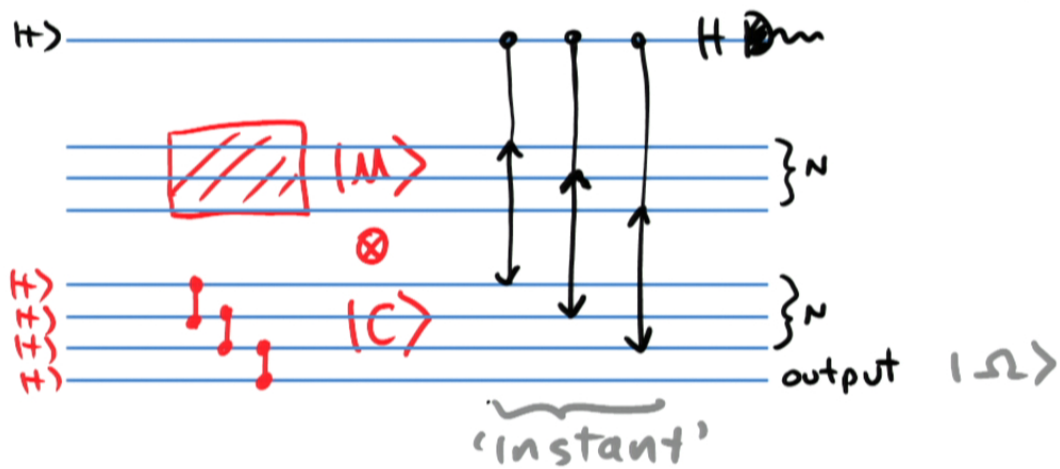


- Q-Sample all measurement records that output $|\Omega\rangle$ [NOT $X|\Omega\rangle$, $Z|\Omega\rangle$ etc]

$|\mu\rangle = |000\cdots0\rangle + \cdots |001101\cdots\rangle + \cdots$ $O(2^n)$ terms

$|\mu\rangle \Rightarrow \cdots + \cdots |\alpha_+\beta_+ - \gamma_- \delta_- \cdots\rangle + \cdots$

$(\Pi_i = |\phi_i\rangle\langle\phi_i|, \ \sum_i |\phi_i\rangle)$

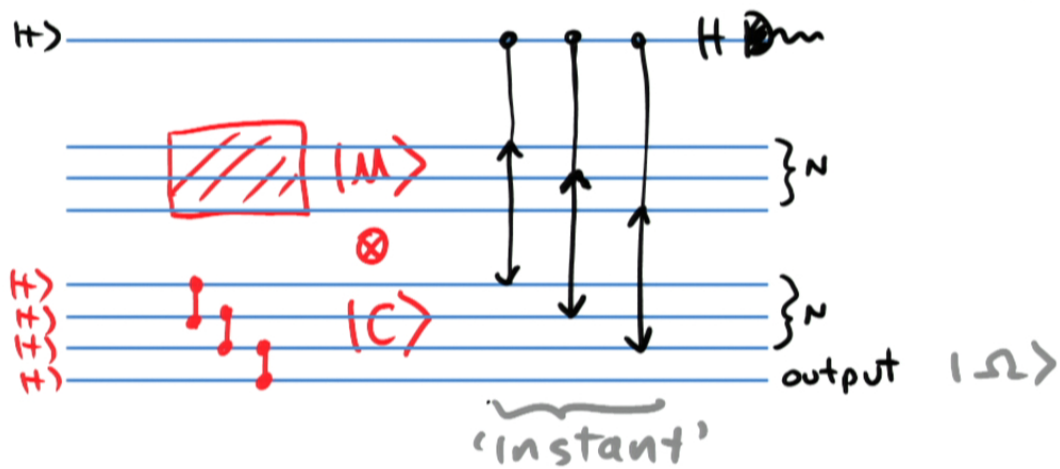


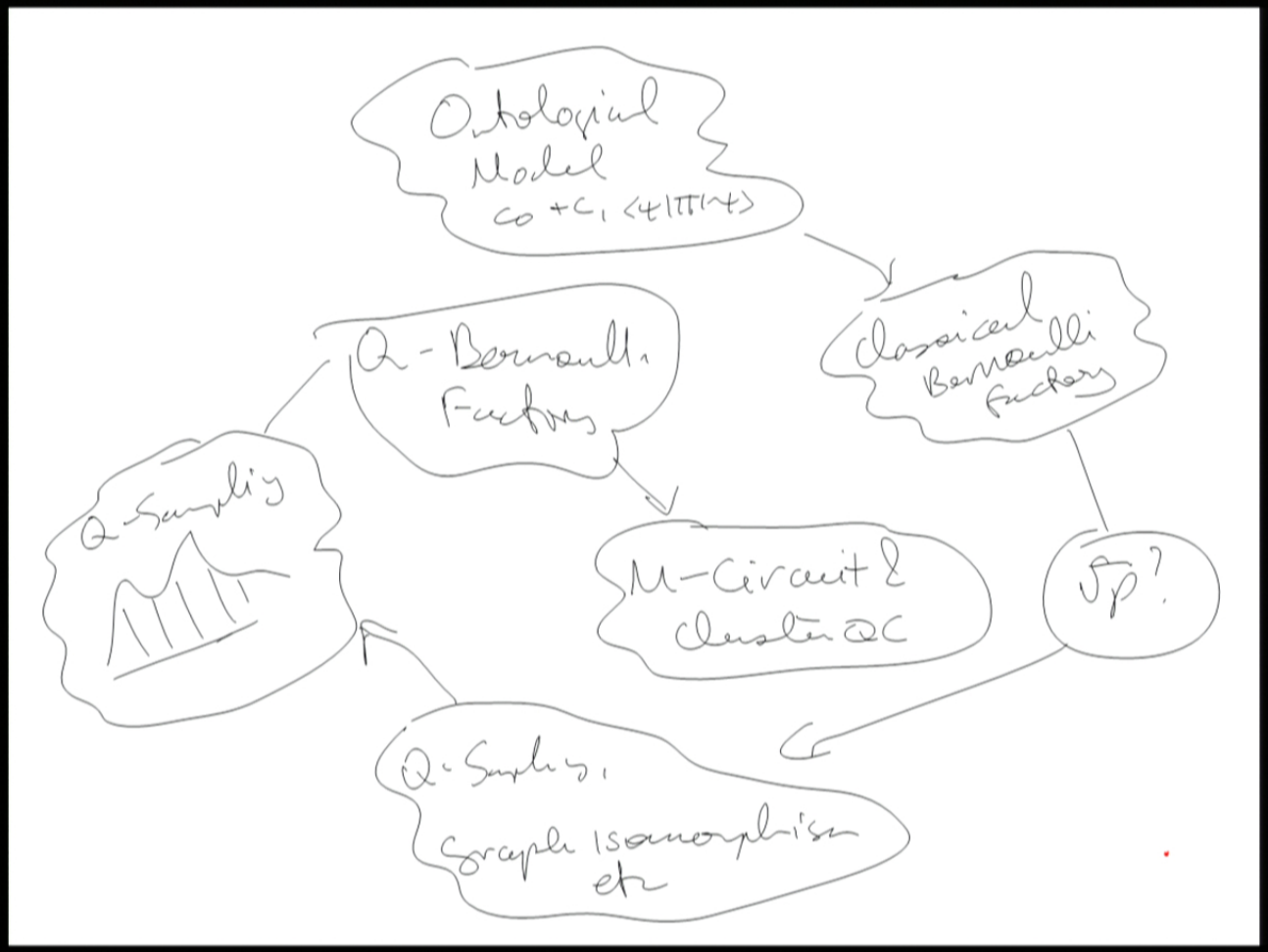
- Q-Sample all measurement records that output $|\Omega\rangle$ [NOT $X|\Omega\rangle$, $Z|\Omega\rangle$ etc]

$$|\mu\rangle = |000\cdots0\rangle + \cdots |001101\cdots\rangle + \cdots \quad O(2^n) \text{ terms}$$

$$|\mu\rangle \Rightarrow \cdots + \cdots |\alpha_+ \beta_+ \gamma_- \delta_- \cdots\rangle + \cdots$$

$$\left(\Pi_i = |\phi_i\rangle\langle\phi_i|, \ \sum_i |\phi_i\rangle\right)$$




Ontological Model
$c_0 + c_1 \langle\psi|\Pi|\psi\rangle$
Classical Bernoulli Factory
Q-Bernoulli Factory
Q-Sampling
M-Circuit & Cluster QC
$\mathcal{P}_{\bar{p}}$?
Q-Sampling,
Graph isomorphism
etc