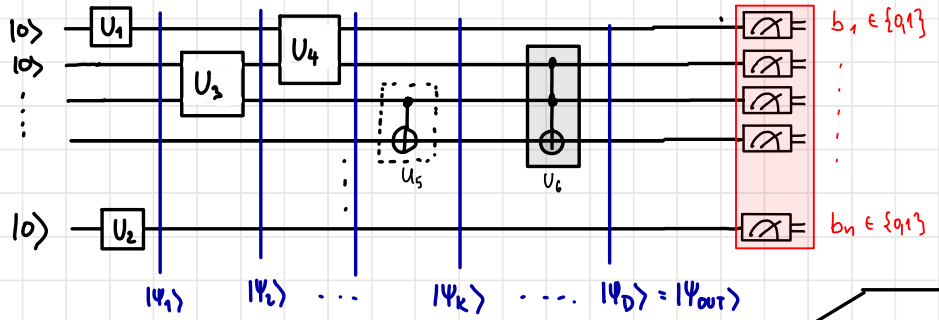
HIGHLIGHTS OF LAST LECTURE:

QUANTUM CIRCUIT

$|\psi_0\rangle = |\psi_{in}\rangle$, e.g.

$|\psi_0\rangle \in (\mathbb{C}^2)^{\otimes n} \cong \mathbb{C}^{2^n}$



MEASUREMENT

$P(b_1 \dots b_n) = |\langle b_1 \dots b_n | \psi_{OUT} \rangle|^2 = |\alpha_{b_1 \dots b_n}|^2$

CIRCUIT EVALUATION

- $2^n \times 2^n$ MATRICES ON 2^n-dim VECTORS

$$|\psi_1\rangle = \left(U_1 \otimes \mathbb{1}_2^{\otimes(n-2)} \otimes U_2\right)|\psi_0\rangle$$
$$|\psi_2\rangle = \left(\mathbb{1}_2 \otimes U_3 \otimes \mathbb{1}_2^{\otimes(n-3)}\right)|\psi_1\rangle$$
$$\vdots$$
$$|\psi_k\rangle = [U_k]\,|\psi_{k-1}\rangle$$

$$|\psi\rangle = \sum_{b_1 \dots b_n \in \{0,1\}^n} \alpha_{b_1 \dots b_n} |b_1 \dots b_n\rangle, \quad \||\psi\rangle\| = 1$$

$U_k \in$ Unitaries / GATE SET G

—— = —[𝟙]— = identity

UNIVERSAL: $G = \{ \text{CNOT} \} \cup \underbrace{U(2)}_{\text{SINGLE-QUBIT } (2\times2) \text{ UNITARIES}}$

APPROX UNIVERSAL: $\tilde{G} = \{ \oplus, H, T \}$, $T = \pi/8$

COMPUT. APPROX UNIVERSAL: $G' = \{ \oplus, H \}$

Q. CIRCUITS: A WAY TO DESCRIBE QUANTUM EVOLUTIONS

	POSTULATES	Q.C. ELEMENTS	MATH (LINEAR ALGEBRA)
1.	STATE SPACE	QUANTUM REGISTER	$\mathbb{C}^{2^n}$
2.	UNITARY EVOLUTION	GATES / SEQUENCE OF	$SU(2)$, $\exp(iH)$ Hermitian operators
3.	MEASUREMENT	READOUT	INNER PRODUCTS, ORTHONORMAL BASIS
4.	COMPOSITE SYSTEMS	QUBIT → REGISTER	TENSOR (KRONECKER) PRODUCT

QUANTUM CIRCUIT ≡ ONE FIXED FUNCTION / MAP

? QUANTUM ALGORITHM* ?

* "QUANTUM ALGORITHM", I BELIEVE IS A MISNOMER. "ALGORITHM FOR QUANTUM COMPUTERS" IS CORRECT.

COMPUTABILITY & (COMPUTATIONAL) COMPLEXITY THEORY

- A PROBLEM IS COMPUTABLE IF ∃ A TURING MACHINE THAT SOLVES IT

  - TURING MACHINES
  - BOOLEAN CIRCUITS*
  - TWO-STACK AUTOMATA
  - CELULAR AUTOMATA
  - λ-CALCULUS
  - GÖDEL-(GENERAL-, μ-) RECURSIVE FUNCTIONS

  } FORMALIZATIONS – MODELS – OF COMPUTATION

ALL CAPABLE OF SOLVING *THE SAME SET OF PROBLEMS* [GÖDEL-TURING-CHURCH]

CHURCH-TURING THESIS

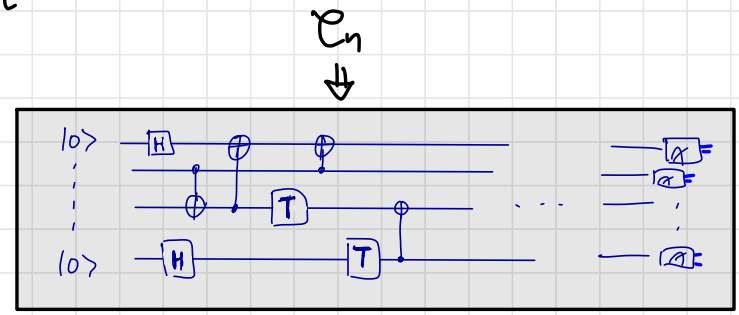
EVERY COMPUTABLE FUNCTION IS COMPUTABLE ON A (DETERMINISTIC) TURING MACHINE

← KNOW THIS

QUANTUM COMPUTATION - CIRCUIT MODEL (1)

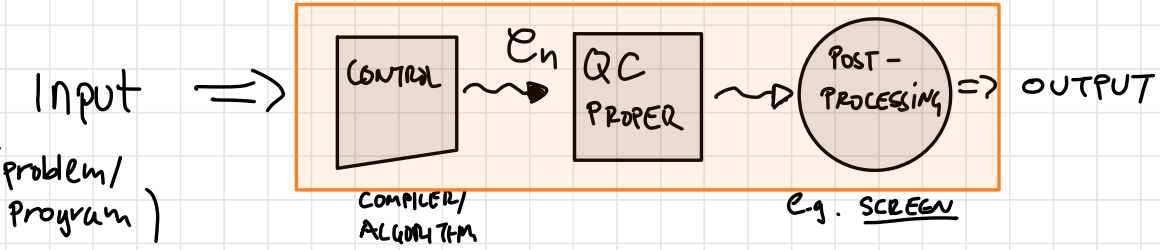
(1.) A DEVICE THAT CAN EXECUTE A CIRCUIT $\mathcal{C}_n$ (on $|\vec{0}\rangle$) & RETURN MEASUREMENT OUTCOME

"Q.C. PROPER"



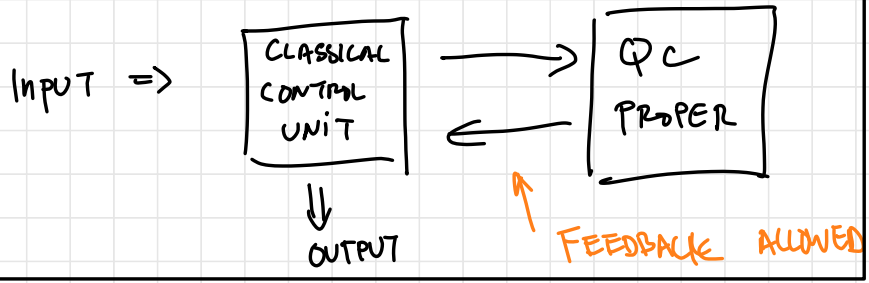
(2.) A CLASSICAL (QUANTUM) DEVICE ON WHICH WE CAN RUN ALGORITHMS / PROGRAMS

QUANTUM COMPUTER



QUANTUM COMPUTATION - CIRCUIT MODEL (2)

(3.) SEEMINGLY MORE GENERALLY

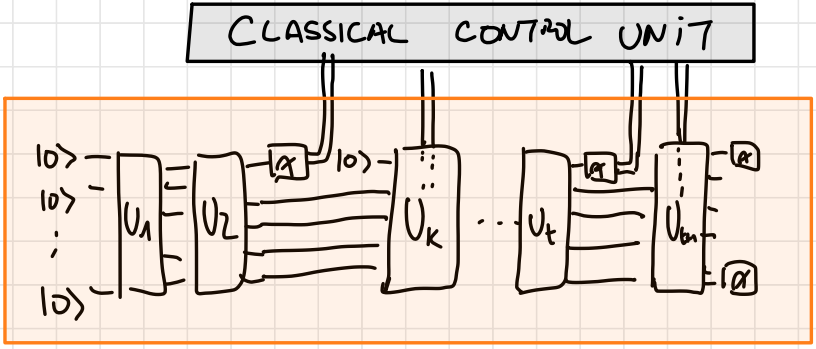


CAN BE MORE CONVENIENT, EFFICIENT, BUT

(2)-(3) & (4) = SAME COMPUTING POWER

(4) EVEN MORE GENERALLY : ADAPTIVE CIRCUITS

QC PROPER:



NOT ALL PROBLEMS ARE COMPUTABLE (SEE HALTING PROBLEM & HILBERT/ACKERMANN'S ENTSCHEIDUNGSPROBLEM)

CAN THE QC MODEL DO BETTER ?

CAN QC's DO BETTER ?

$f: \{0,1\}^* \to \{0,1\}^*$

NO. EVERY PROBLEM SOLVABLE ON A QC IS SOLVABLE ON A CC (WITH RANDOM COIN)

FURTHERMORE: A QC CAN COMPUTE ALL FUNCTIONS A CC CAN

THEOREM: $CC = QC^*$

* CC(QC) = SET OF PROBLEMS SOLVABLE ON CC (QC)

Soo.. WHY CARE ABOUT QC? IN A SEC.

PROOF: PROVE $CC \subseteq QC$ & $QC \subseteq CC$.

a) $CC \supseteq QC$

- SIMULATE "QC PROPER": ITS JUST MULTIPLICATION OF MATRICES & VECTORS TO GET TO $[|\psi_{OUT}\rangle]$ (albeit, large!)

  $[\cdot]$:= NUMERICAL REPRESENTATION OF

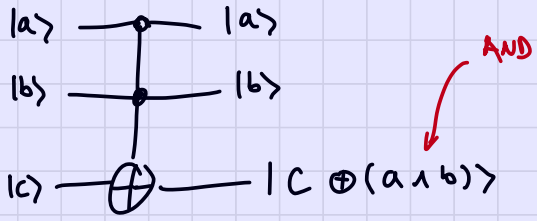
- ONCE GET $[|\psi_{OUT}\rangle]$ CAN USE REJECTION SAMPLING, OR OTHER RANDOMIZED ALGORITHMIC METHODS TO SAMPLE FROM $P_{|\psi_{OUT}\rangle}(b_1 .. b_n)$ (need coin for this! ↓ Randomness)

b) QC ⊇ CC

IN DETAIL:

$\forall$ CLASSICAL CIRCUIT C^{cc}_n COMPUTING $f: \{0,1\}^n \to \{0,1\}^m$

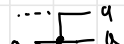
$\exists$ QUANTUM CIRCUIT $C^{QQ}_L(\vec{x})$ WHICH WHEN RUN ON "QC-PROPER" GIVEN INPUT $\vec{x} \in \{0,1\}$ OUTPUTS THE BITSTRING $f(\vec{x}) \cdot \vec{0}$ WITH PROB. 1



$\Rightarrow$ SET: $c = 1$ $\Rightarrow$ $|a\rangle|b\rangle|1\rangle \to |a\rangle|b\rangle|1 \oplus a \wedge b\rangle$

$= |a\rangle|b\rangle|\text{NAND}(a,b)\rangle$

TAKE A CLASSICAL CIRCUIT, REPRESENT IN (NAND + FANOUT (COPY))

- FANOUT ← CNOT  $\Rightarrow$ CNOT $|a\rangle|0\rangle = |a\rangle|a\rangle$
- NAND ← TOFFOLI (+ 1 ANCILLA / AUXILIARY QUBIT)

TOFFOLI IS A 3-QUBIT UNITARY

8×8 MATRIX

n-bit m-NAND k-FANOUT

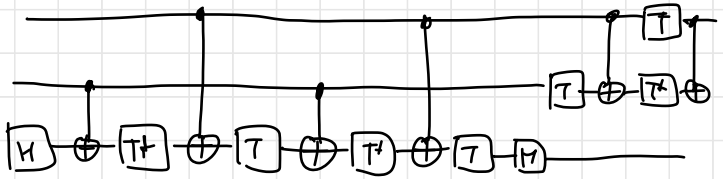
$\Rightarrow$ $m + k + n$ QUBITS

m-TOFFOLI

k-CNOTS

FOR THOSE WHO JUST... CRAVE... MORE INFO:

- TOFFOLI CAN BE IMPLEMENTED FROM $\{CNOT, \pi/8, H\}$



- - - -

- BUT CANNOT BE IMPLEMENTED FROM JUST $\oplus$ & H ..

($\oplus$ + H) IS QC-STRONG ;

$\oplus$ IS CC-STRONG ;

$\oplus$ + H + PAULI + S IS WEAKER THAN C.C.

"CLIFFORD GATE SET"

.. = $\oplus$L ("PARITY-L")

($\oplus$ + H + $\pi/8$) IS QC-STRONG

COMPUTABILITY-WISE ... QC = CC

WHAT ABOUT HOW FAST... HOW EFFICIENTLY THEY COMPUTE?

ENTER COMPLEXITY THEORY.

COMPLEXITY THEORY

→ COMPLEXITY OF AN **ALGORITHM**

THINK: $n \xrightarrow{\mathcal{A}} C_n$

- GATE COMPLEXITY = $n \longmapsto |\mathcal{A}(n)|$

  ↑ # gates as a function of input size

  c.f. "TIME COMPLEXITY"

- SPACE COMPLEXITY = $n \longmapsto$ # Qubits OF CIRCUIT

  CATCH = - OFTEN NEED ANCILLAS

  - LOGSPACE!

TIME & SPACE COMPLEXITY LIVE NATURALLY IN THE TURING MACHINE MODEL OF COMPUTATION... BUT MAP EASILY TO CIRCUIT MODELS

COMPLEXITY THEORY

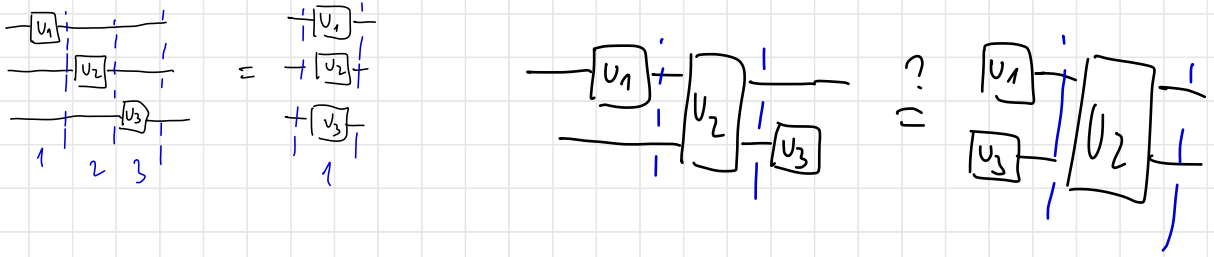
→ COMPLEXITY OF AN **ALGORITHM**

THINK:

$n \xmapsto{\mathcal{A}} C_n$

- DEPTH COMPLEXITY $n \longmapsto \text{LAYERS}(\mathcal{A}(n))$

  ... MINIMAL NUMBER OF LAYERS .. COMMUTATIVITY AN ISSUE



- DEPTH COMPLEXITY A NATIVELY CIRCUIT-MODEL MEASURE ... HAS TO DO WITH PARALLELIZATION!
- DECOHERENCE? "EXPERIMENT COHERENCE TIME"

COMPLEXITY THEORY

Complexity usually expressed IN "BIG-O" NOTATION

e.g. $0.3n^3 + \sqrt{2}n^2 \in O(n^3)$

DEF: $f(n) \in O(g(n))$ $\exists k>0$ $\exists n_0>0$ st. $\forall n>n_0$ $|f(n)| < k \cdot g(n)$ • (approx...)

↑ upper bound

$f(n) \in \Omega(g(n))$ $\exists k>0$ $\exists n_0>0$ st $\forall n>n_0$ $f(n) \geq k \cdot g(n)$

$f(n) \in \Theta(g(n))$ $f(n) \in O(g(n))$ & $f(n) \in \Omega(g(n))$

WE WILL MOSTLY CARE ABOUT $O(poly(n))$ & $O(exp(n))$

↑ "SOME POLYNOMIAL"

Complexity classes

A complexity class $\mathcal{C}$ is

a set of problems (with "size" n) which can be solved on a machine/model M using $O(f(n))$ of resource $\mathbb{R}$

Ex. Computable_{TM} = all problems solvable on a TM using $f(n)$ time, for any function $f : \mathbb{N} \to \mathbb{N}$, $f < \infty$

We know:

$$\text{Computable}_{TM} = \text{Computable}_{QC}$$

COMPLEXITY CLASSES

SMALL COMMENT ...

WHAT IS A "PROBLEM" HERE?

FOR NOW DECISION PROBLEMS

= PROBLEMS WITH YES/NO ANSWER

PROBLEM (LANGUAGE) $L_{YES} \subseteq \{0,1\}^*$ $L_{NO} \subseteq \{0,1\}^*$ $L_{NO} = \{0,1\}^* \setminus L_{YES}$, OR "PROMISE"

$\vec{x} \in L_Y \cup L_{NO}$

IS $x \in L_{YES}$?

COMPLEXITY CLASSES

A SET OF PROBLEMS (WITH "SIZE" n) WHICH CAN BE SOLVED ON A MACHINE/MODEL M USING $O(f(n))$ OF RESOURCE R

SOME FAMOUS EXAMPLES:

P = DECISION PROBLEMS (YES/NO) SOLVABLE ON A DETERMINISTIC TURING MACHINE IN $O(\text{poly}(n))$ TIME

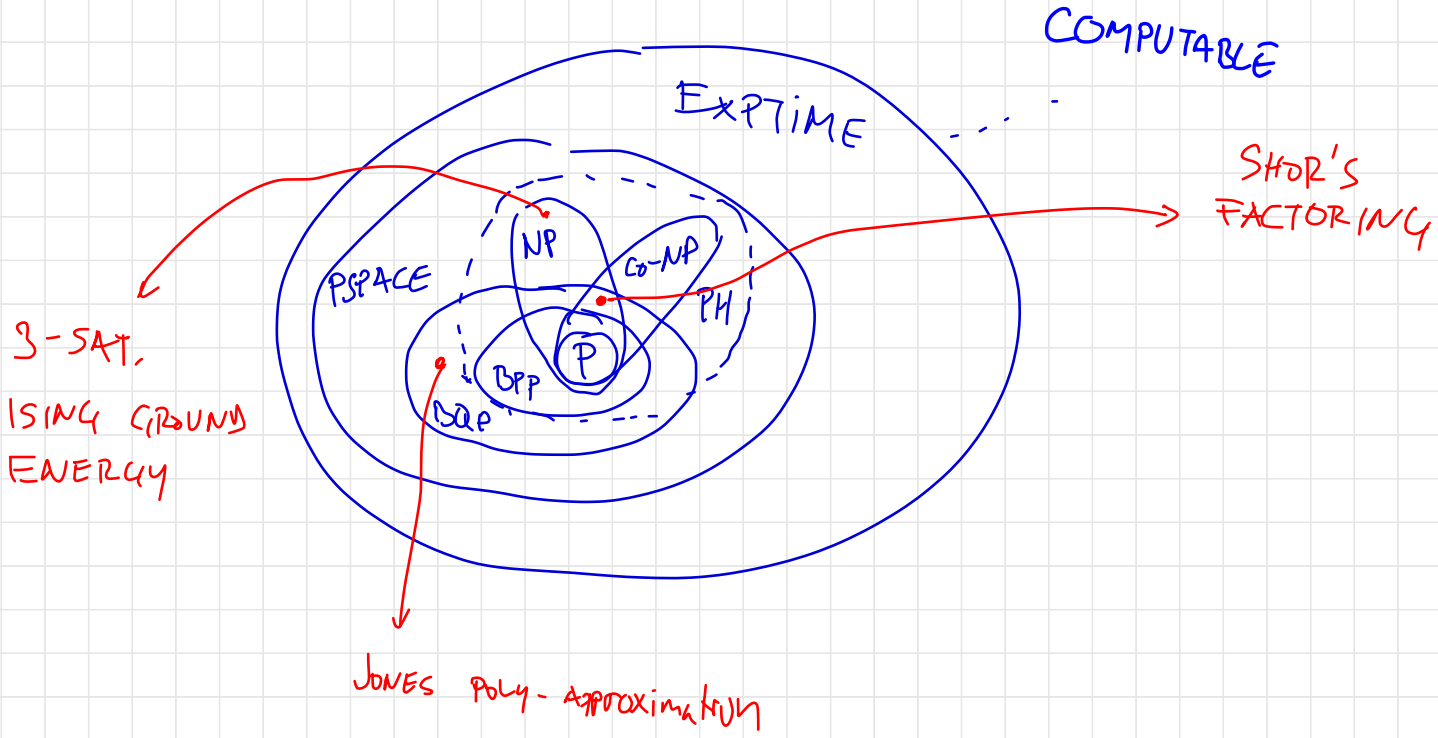
BPP = PROBABILISTIC TM, $O(\text{poly}(n))$, TIME, BOUNDED ERROR

NP = NON-DETERMINISTIC TM, $O(\text{poly}(n))$, TIME

BQP = QUANTUM TM (CIRCUITS), $O(\text{poly}(n))$, TIME

PSPACE = DETERMINISTIC TM, $O(\text{poly}(n))$, SPACE

EXPTIME = ...



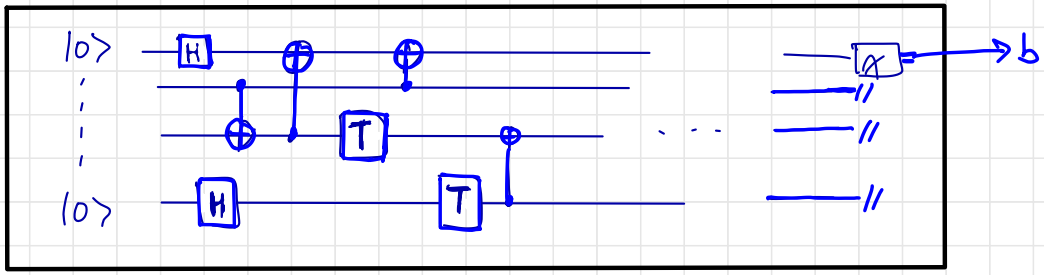
SO WHAT IS A "BQP" PROBLEM EXACTLY?

$\vec{x} \in L = L_{YES} \cup L_{NO} \subseteq \{0,1\}^*$

$\vec{x}$ ENCODES AN ISTANLE OF YES/NO QUESTION ... $|\vec{x}| = n$

BQP: $\exists$ POLY-TIME TM. A : $\vec{x} \to \boxed{A} \to \mathcal{C}_n^Q$

$\mathcal{C}_n$ GOES INTO "QC-PROPER" (NOTE $|\mathcal{C}_n^Q| \in O(\text{poly}(n))$)



IF $\vec{x} \in L$ THEN $P(b=1) \geq \frac{2}{3}$

IF $\vec{x} \notin L$ THEN $P(b=1) \leq \frac{1}{3}$

$(P(b=0) \geq \frac{2}{3})$

ARBITRARY CONSTANTS. $1/2 + \frac{1}{\text{poly}(n)}$ is ok.

CLASSICAL COMPUTERS CAN SIMULATE QUANTUM COMPUTERS WITH AN EXPONENTIAL SLOWDOWN.

KNOWN: $L \subseteq P \subseteq NP \subseteq PSPACE$ & $L \subset PSPACE$

$BPP \subseteq BQP \subseteq PP \subseteq PSPACE$

$BPP \subseteq PH$

BQP vs PH? UNLIKELY. —

NP := PROBLEMS VERIFIABLE IN POLY-TIME ON DET. TURING M.

- COMPLETE PROBLEMS & REDUCTIONS

STRONGLY BELIEVE:

$P \neq NP$.

$BQP \neq BPP$

$BQP \not\supseteq NP$

TRIVIAL: $P \subseteq NP$

$P \subseteq BPP \subseteq BQP$

P VS. NP THE BIGGEST ($\$10^6$) QUESTION IN (T) CS

BPP VS. BQP ... IN QCS

(VERY STRONG EVIDENCE IN BOTH CASES)

BUT IT COULD BE $P = PSPACE$

$P = BPP = NP = BQP = PSPACE$

ALSO:

"POLYNOMIAL HIERARCHY (PH) DOES NOT COLLAPSE..."

$P \subseteq NP \subseteq NP^{NP} \subseteq NP^{NP^{NP}} \subseteq NP^{\cdots} \cdots \subseteq PSPACE$

N.B. $P = NP \Rightarrow$ FULL COLLAPSE

IMPORTANT IN "QUANTUM SUPREMACY"

CHURCH-TURING THESIS

=> EXTENDED (STRONG) CHURCH-TURING THESIS (BERNSTEIN & VAZIRANI)

CAN BE BUILT

ANY REALISTIC MODEL OF COMPUTATION IS EFFICIENTLY SIMULATABLE BY A PROBABILISTIC TURING MACHINE

poly-resources

BQP ≠ BPP WOULD VIOLATE THIS

MUCH OF Q. COMPLEXITY THEORY USED TO BE ABOUT DECISION PROBLEMS...

- SEARCH (OR FUNCTIONAL) PROBLEMS
- COUNTING PROBLEMS
- SAMPLING PROBLEMS ← STRONG SEPARATION RESULTS (COM. THEO ASSUMPT.) → "QUANTUM SUPREMACY"
- ORACULAR PROBLEMS ← UNCONDITIONAL SEPARATIONS (PROMISE)

GETTING "IN THE GROOVE" WITH BASIC

Q. ALGOS & MAIN PROPERTIES...

EXAMPLE 1. DEUTSCH-JOZSA

$f : \{0,1\}^n \to \{0,1\}$

PROMISE : f is CONSTANT OR BALANCED

DECIDE WHICH.

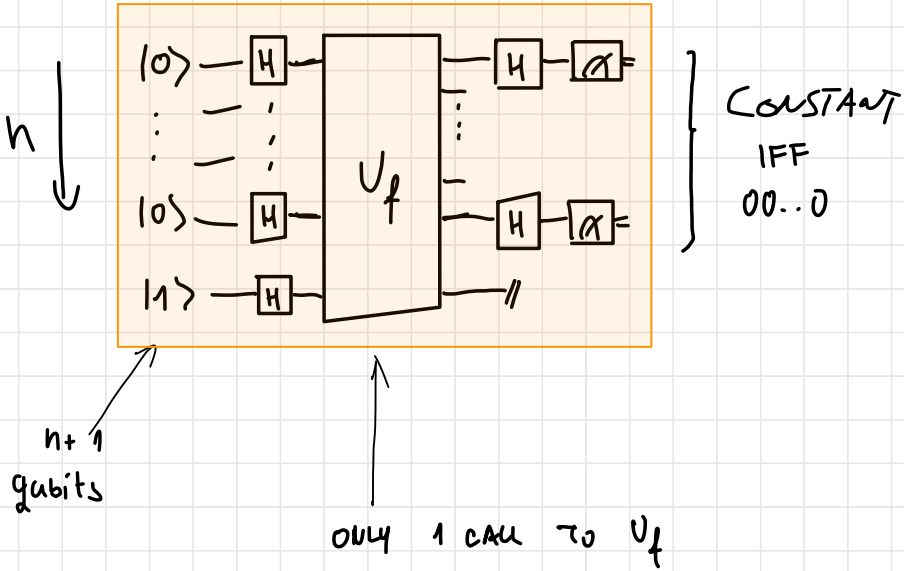
QUANTUM ACCESS :

"BIT-FLIP ORACLE"

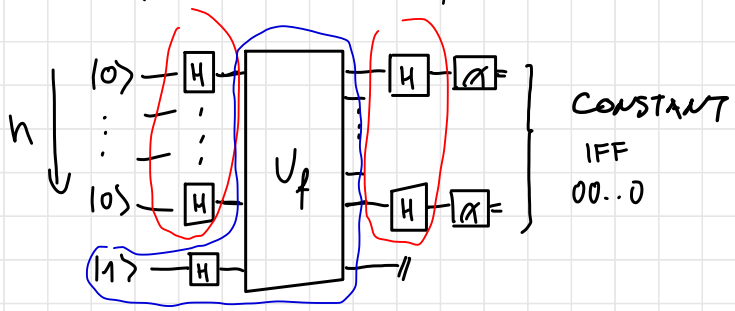
$f \to U_f |\vec{x}\rangle|b\rangle = |\vec{x}\rangle|b \oplus f(\vec{x})\rangle$

QUANTUM ALGORITHM

INSTANCE SIZE n



QUANTUM ALGORITHM (instance size n)



Q. ALGO. TRICKS:

- "UNIFORM SUPERPOSITION PREPARATION" (& MEASUREMENT) $H^{\otimes n}|0\rangle = \frac{1}{\sqrt{2^n}}\sum|b_1 \dots b_n\rangle$

- "PHASE KICK-BACK"

$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) =: |-\rangle$; $\mathrm{CNOT}|b\rangle|-\rangle = (-1)^b|b\rangle|-\rangle$

PHASE KICKS BACK

$\Rightarrow U_f|\vec{x}\rangle|-\rangle = (-1)^{f(\vec{x})}|\vec{x}\rangle|-\rangle$ PHASE FLIP ORACLE

STATE AFTER ORACLE:

$$\left(\frac{1}{\sqrt{2^n}}\sum_{\vec{x}}(-1)^{f(\vec{x})}|\vec{x}\rangle\right)\otimes|-\rangle;$$

DEF: $|\psi\rangle = \frac{1}{\sqrt{2^n}}\sum_{\vec{x}}(-1)^{f(\vec{x})}|\vec{x}\rangle$ → CONST / BAL !

$P(0\cdots0) = |\langle 0\cdots0|H^{\otimes n}|\psi\rangle|^2$

$\propto [1,1,1\dots1] \cdot \begin{bmatrix}\alpha_1\\ \vdots\\ \alpha_{2^n}\end{bmatrix} \propto \sum\alpha_i$

BALANCED = 0

CONSTANT −1 or +1

⇨ DESTRUCTIVE INTERFERENCE !

$$H|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$$

$$H|1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right)$$

$$H^{\otimes 4}|0\ldots0\rangle = \frac{1}{\sqrt{2^4}} \bigotimes \left(|0\rangle + |1\rangle\right)$$

CLASSICAL LOWER BOUNDS.

- DETERMINISTIC TM / CIRCUIT WORST CASE: $\Omega(2^{n-1})$ CALLS

  $\Rightarrow$ EXPONENTIAL SEPARATION

- RANDOMIZED (PROBABILISTIC) CONSTANT (BOUNDED) ERROR: $O(1)$ $\Rightarrow$ NO SEPARATION

  (WITHIN $\varepsilon > 0$ ERROR, $O(\log(1/\varepsilon))$)

THIS MEANS "SOME CONSTANT NUMBER OF CALLS" E.G. 5 (DEPENDING ON YOUR B.E. PROBABILITY)

EXAMPLE 2

SIMON'S PROBLEM $f : \{0,1\}^n \to \{0,1\}^n$ PROMISE $\exists\ \vec{s} \in \{0,1\}^n$

s.t. $f(\vec{x}) = f(\vec{y}) \iff \vec{x} \oplus_2 \vec{s} = \vec{y}$

Given O_f FIND $\vec{s}$

QUANTUM ORACLE $U_f |\vec{x}\rangle |\vec{b}\rangle = |\vec{x}\rangle |\vec{b} \oplus_2 f(\vec{x})\rangle$

↑ POINT-WISE XOR

$(x_1, x_2 \dots x_n) \oplus_2 (y_1, y_2 \dots y_n) = (x_1 \oplus y_1, x_2 \oplus y_2, \dots, x_n \oplus y_n)$

EXAMPLE 2

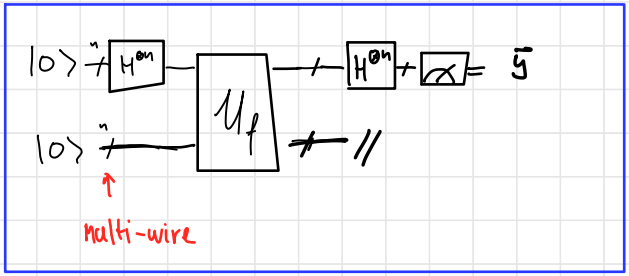
SIMON'S PROBLEM $f : \{0,1\}^n \to \{0,1\}^n$ PROMISE $\exists\ \vec{s} \in \{0,1\}^n$

s.t. $f(\vec{x}) = f(\vec{y}) \iff \vec{x} \oplus_2 \vec{s} = \vec{y}$

Given O_f FIND $\vec{s}$

QUANTUM $U_f |\vec{x}\rangle|\vec{b}\rangle = |\vec{x}\rangle|\vec{b} \oplus_2 f(\vec{x})\rangle$

CIRCUIT



IF $\vec{s} = 0..0$ $\vec{y}$ is FULLY RANDOM

IF $\vec{s} \neq 0..0$ $\vec{y}$. st. $\vec{y}.\vec{s} = 0$ (in $\mathbb{F}_2$)

& UNIFORM

COMPLETE ALGORITHM

1) REPEAT $\mathcal{C}$ n TIMES, WITH $P \geq 0{,}28\ldots$

$\vec{y}_1 .. \vec{y}_{n-1}$ ARE LIN INDEP IN $\mathbb{F}_2$

[1.5) GOTO 1 IF NOT LIN. INDEP. OR GOTO 1 $\log(1/\varepsilon)$ time]

2) SOLVE $\vec{y}_1.\vec{s} = 0$, $\vec{y}_2.\vec{s} = 0$, ⋮, $\vec{y}_{n-1}.\vec{s} = 0$ IN $\mathbb{F}_2$ TO YIELD $\vec{s}$.

VER 1. "REPEAT UNTIL SUCCESS" (LAS VEGAS)
$O(n)$ EXPECTED CALLS

VER 2. "FAIL WITH PROB ε" (MONTE CARLO)
$O(n \log(1/\varepsilon))$ CALLS

LET'S WORK IT OUT ... ASSUME $\vec{s} \neq \vec{0}$

AFTER $H^{\otimes n}$: $\propto \sum_{\vec{x} \in \{0,1\}^n} |\vec{x}\rangle |0\rangle$

AFTER ORACLE: $\propto \sum_{\vec{x}} |\vec{x}\rangle |f(\vec{x})\rangle$

Inner product OF BITSTRINGS in $\mathbb{F}_2$ (mod 2)

NOTE: $H^{\otimes n} |\vec{x}\rangle \propto \sum_{\vec{y}} (-1)^{\vec{x} \cdot \vec{y}} |\vec{y}\rangle$

AFTER $H^{\otimes n}$: $\propto \sum_{\vec{x}} \sum_{\vec{y}} (-1)^{\vec{x} \cdot \vec{y}} |\vec{y}\rangle |f(\vec{x})\rangle$

BEFORE MEASUREMENT : $\propto \sum_{\vec{x}} \sum_{\vec{y}} (-1)^{\vec{x}\cdot\vec{y}} |\vec{y}\rangle |f(\vec{x})\rangle$

FINALLY $P(y) \propto \| \sum_{\vec{x}} (-1)^{\vec{x}\cdot\vec{y}} |f(\vec{x})\rangle \|^2 \propto \| \sum_{z \in RANGE(f)} (-1)^{\vec{x}\cdot\vec{y}} + (-1)^{(\vec{x}\oplus\vec{s})\cdot\vec{y}} |z\rangle \|^2$

"z"

$(\vec{x}\oplus\vec{s})\cdot\vec{y} = \vec{x}\cdot\vec{y} \oplus \vec{s}\cdot\vec{y}$

$= \| \sum (-1)^{\vec{x}\cdot\vec{y}} \underbrace{(1 + (-1)^{\vec{s}\cdot\vec{y}})}_{} |z\rangle \|$

Ø UNLESS $\vec{s}\cdot\vec{y} = 0$.

EXAMPLE 2

SIMON'S PROBLEM $f : \{0,1\}^n \to \{0,1\}^n$ PROMISE $\exists\ \vec{s} \in \{0,1\}^n$

s.t. $f(\vec{x}) = f(\vec{y}) \iff \vec{x} \oplus_2 \vec{s} = \vec{y}$

Given O_f FIND $\vec{s}$

TH (SIMON) ANY CLASSICAL ALGORITHM NEEDS $\Omega(2^{n/2})$ CALLS (WITH OR WITHOUT RANDOMNESS) TO SOLVE S.P. WITH NON-NEGLIGIBLE PROBABILITY.

QUANTUM : $O(n)$ ——— EXPONENTIAL SEPARATION ——— CLASSICAL : $\Omega(2^{n/2})$

RELATIVE TO THIS ORACLE (NOT ABOUT BPP vs BPP)

COMMENT: • IS SIMON'S ALGORITHM "A QUANTUM ALGORITHM"
• A "HYBRID ALGORITHM"?

→ FOR PRACTICAL PURPOSES WE LIKE HYBRID ALGOS
WHICH SPECIFY CLASSICAL & QUANTUM PARTS
MORE CLASSICAL IS BETTER

→ FOR (MOST) THEORY, RECALL CC ⊆ QC ...
I CAN MAKE ALL CLASSICAL PARTS QUANTUM

CF ALSO "PRINCIPLE OF DEFERRED/DELAYED MEASUREMENT"
= ALL MEASUREMENTS CAN BE "PUSHED TO THE END"

SO FAR ONLY "ORACULAR" SETTINGS ...

CAN WE GET "NATURAL", END-TO-END ADVANTAGES.

YES, BUT IT IS NOT EASY.

EXAMPLE 3... A "FULLY QUANTUM" ALGORITHM

QUANTUM FOURIER TRANSFORM.

- FOURIER TRANSFORM (WATCH 3BROWN1BLUE ON YOUTUBE!)

  → EXPRESSING A PERIODIC FUNCTION $f(x)$ AS A SERIES IN $\phi_k(x) = \exp\left(i \frac{k\pi x}{L}\right)$ ON $[-L, L]$

  → INVALUABLE IN THEORY AND APPLICATION.

- DISCRETE F.T. $\vec{x} = (x_1 \dots x_N)$

  $\vec{y} = DFT(\vec{x})$ DEF WITH

$$y_k = \sum_{\ell=0}^{N-1} x_\ell \exp\left(-i\, 2\pi \frac{k\ell}{N}\right)$$

  => LINEAR MAP: $(DFT)_{k\ell} = \exp\left(-i\, 2\pi \frac{k\ell}{N}\right)$

  ORTHOGONAL COLUMNS...
  BUT NOT ORTHONORMAL

DFT CAN BE MADE UNITARY:

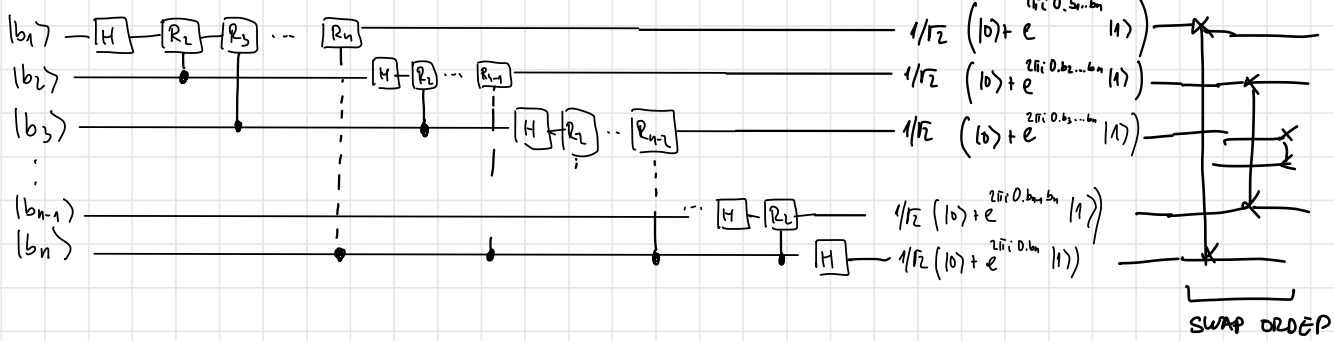
$$\mathcal{U}DFT = \frac{1}{\sqrt{N}} DFT$$

CLASSICAL COST: - NAÏVE $O(N^2)$
- FAST F.T. $O(N \log(N))$

APPLICATIONS:
- SIGNAL PROCESSING
- COMPRESSION
- MACHINE LEARNING (E.G. JOHNSON-LINDENSTRAUSS TRANSFORM AND UNSUPERVISED LEARNING (DIM. REDUCTION))
- FFT-BASED MULTIPLICATION OF POLYNOMIALS
- FFT-BASED MULTIPLICATION OF INTS (SCHÖNHAGE-STRASSEN ALGO)

... BUT UDFT IS Unitary .. VALID QUANTUM OPERATION

$\Rightarrow \exists$ CIRCUIT ... LET $N = 2^n$ ... QFT



$QFT|b_1 \ldots b_n\rangle$

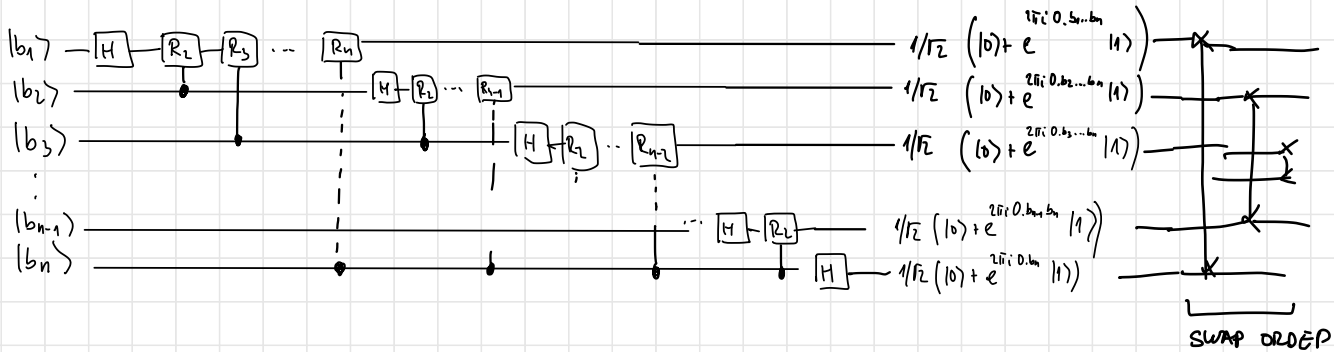
$$R_k = \begin{pmatrix} 1 & 0 \\ 0 & \exp(2\pi i / 2^k) \end{pmatrix}$$

THIS CIRCUIT HAS A NICE, INFORMATIVE CONSTRUCTION & LOGIC

SEE N&C OR MY LECTURE NOTES (LESSON 4)

... BUT uDFT IS Unitary .. VALID QUANTUM OPERATION.

⇒ ∃ CIRCUIT ... LET $N = 2^n$ ... QFT



$QFT|b_1 \ldots b_n\rangle$

QFT TASK : INPUT : Q. STATE $|\psi\rangle$

OUTPUT : Q STATE $uDFT|\psi\rangle$

QFT ALGORITHM $O(n^2)$ [appx : $O(n \log n)$]

CLASSICAL FFT $O(2^n \times n)$

} EXPONENTIAL BUT APPLES & ORANGES

IF PERFORMS uDFT ON AMPLITUDES

NOT DIRECTLY ACCESIBLE

MUST BE SNEAKY

SNEAK PART 1.

QUANTUM PERIOD FINDING

ONLY INTUITION ...

ASSUME $f: \{0,\dots,L-1\} \to \{0,\dots,L-1\}$ IS PERIODIC $(\exists T \text{ ST } f(x)=f(x+T) \ \forall x$ & VALUES BETWEEN DISTINCT ...

FOR TECHNICAL REASONS, $L = 2^k$, $T < \frac{\sqrt{L}}{2}$

- HAVE U_f, $U_f|x\rangle|y\rangle = |x\rangle|y +_L f(x)\rangle$

FIND T in $\text{poly}(k) = \text{polylog}(L)$ (CLASSICALLY?)

ALGO:

1) PREPARE $|\psi\rangle = \frac{1}{\sqrt{L}} \sum_{x=0}^{L-1} |x\rangle_1 |f(x)\rangle_2$ (HOW?)

2) (OPTIONAL) MEASURE REG 2

3) APPLY QFT ON REG 1

4) APPLY CONTINUED FRACTIONS ALGORITHM TO FIND T

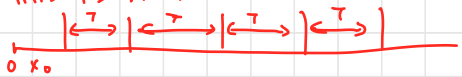
1) PREPARE $|\psi\rangle = \frac{1}{\sqrt{L}} \sum_{x=0}^{L-1} |x\rangle_1 |f(x)\rangle_2$

2) (OPTIONAL) MEASURE REG 2 $\Rightarrow$ GET $y_0 = f(x_0)$ WITH UNIFORM PROB OVER RANGE
↳ smallest x st $f(x) = y$

$$|\psi_0\rangle = \frac{1}{\sqrt{\left[\frac{L}{T}\right]}} \sum_{t=0}^{\left[\frac{L}{T}\right]-1} |x_0 + tT\rangle |f(x_0)\rangle$$

↑ all x st $f(x) = y_0$

THIS IS A "PERIODIC STATE"



3) APPLY QFT ON REG 1

QFT TRANSFORMS "PERIODIC STATES"
TO OTHER PERIODIC STATES

$\simeq k \times \frac{L}{L \times T} = \frac{k}{T}$ FOR SOME k

4) a) IF EXACT $(T|L)$ DO TWICE; $\frac{k}{T}, \frac{k'}{T}$ $\left(= \frac{a}{b}, \frac{a'}{b'}\right.$ SIMPLIFIED$\left.\right)$
IF $GCD(k, T)$ & $GCD(k', T)$ ARE COPRIME (OFTEN ARE)
$T = LCM(b, b')$

b) IF $\frac{L}{T} \notin \mathbb{Z}$ THEN APPLY CONTINUED FRACTIONS ALGO DISTILLS EXACT WITH HIGH PROB. EFFICIENTLY

PERIOD-FINDING IS EXPONENTIALLY MORE EFFICIENT
BUT AGAIN ORACULAR...

THEOREM (SHOR)

LET N BE AN INPUT INTEGER.

IF WE FIND THE PERIOD OF $f_a^N(x) = a^x \bmod N$, FOR A CHOSEN a

WE CAN FIND THE FACTORS OF N EFFICIENTLY

ALSO: $\exists$ EFFICIENT CIRCUIT TO CONSTRUCT U_f FOR f_a^N, FOR ANY a, N.

COR: $\mathcal{Q}\mathcal{C}$ CAN FACTOR NUMBERS EFFICIENTLY

ALSO: "SHOR'S ALGO IS A DE-ORACULIZATION OF PERIOD-FINDING" ... KIND OF...

THIS WAS ALL RATHER SNEAKY...

QFT => WHICH ONLY WORKS ON AMPLITUDES, WHO NEEDS THAT?!

↓

PERIOD FINDING => WHICH IS AN ORACULAR ALGORITHM, HOW DO WE ACTUALLY USE THIS? WHERE IS YOUR ORACLE?)

↓ SHOR!

FACTORING => HUH... THIS IS SNEAKY!

BEST KNOWN CLASSICAL ALGORITHM $\tilde{O}\left(\exp\left(\sqrt[3]{\log N}\right)\ldots\right)$ LENSTRA!

SHOR: $\tilde{O}\left(\log^2 N\right)$

BUT... FACTORING IN NP ∩ CO-NP... NOTHING "WEIRD" HAPPENS IF IN BPP...

OK... WE GOT INTO THE GOOVE

BUT DID NOT DISCUSS GROVER

GROVER'S SEARCH IS OPTIMAL...

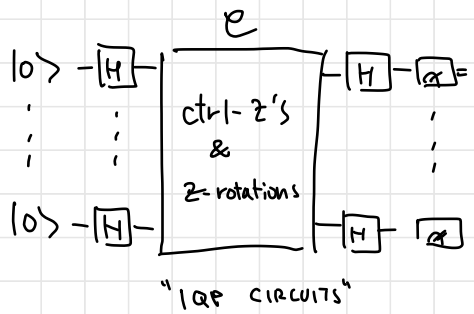
$\Omega(\sqrt{N})_q$ VS $\Omega(N)_c$

LOOK IT UP!

NOT EXPONENTIAL SEPARATION, BUT GENERICALLY USEFUL.

A WORD ON

- SAMPLING PROBLEMS:



$P(b_1 .. b_n)$

TASK:

GIVEN CIRCUIT C GIVE A CLASSICAL RANDOMIZED ALGO OUTPUTTING $b_1 .. b_n$ WITH PROB $P'(b_1 .. b_n)$ WHERE P' IS CLOSE TO P

IF POSSIBLE IN POLY-TIME FOR THE WORST CASE
-- EVEN WITH ADDITIVE CONSTANT ERROR..
PH - COLLAPSES TO 3RD LEVEL.

FACTORING IN BPP HAS NO SUCH REPERCUSSIONS...

- SAMPLING CAN BE <u>PROVABLY HARD</u> (UP TO SIGNIFICANT COMPLEXITY-THEORETIC REPERCUSSIONS) FOR RELATIVELY SIMPLE COMPUTATIONS / MODELS

- QUANTUM SUPREMACY: EXHIBITING SUCH A PROVABLY HARD COMPUTATION

NO MATTER HOW USELESS.

WE KNOW

$$FBPP = FBQP \iff SAMP\,BPP = SAMP\,BQP$$

$$SAMP\,BPP = SAMP\,BQP \implies BQP = BPP$$

BUT

$$BQP = BPP \not\Longrightarrow SAMP\,BPP = SAMP\,BQP$$

?

EXACT $SAMP\,BPP = SAMP\,BQP \implies$ PH - COLLAPSE