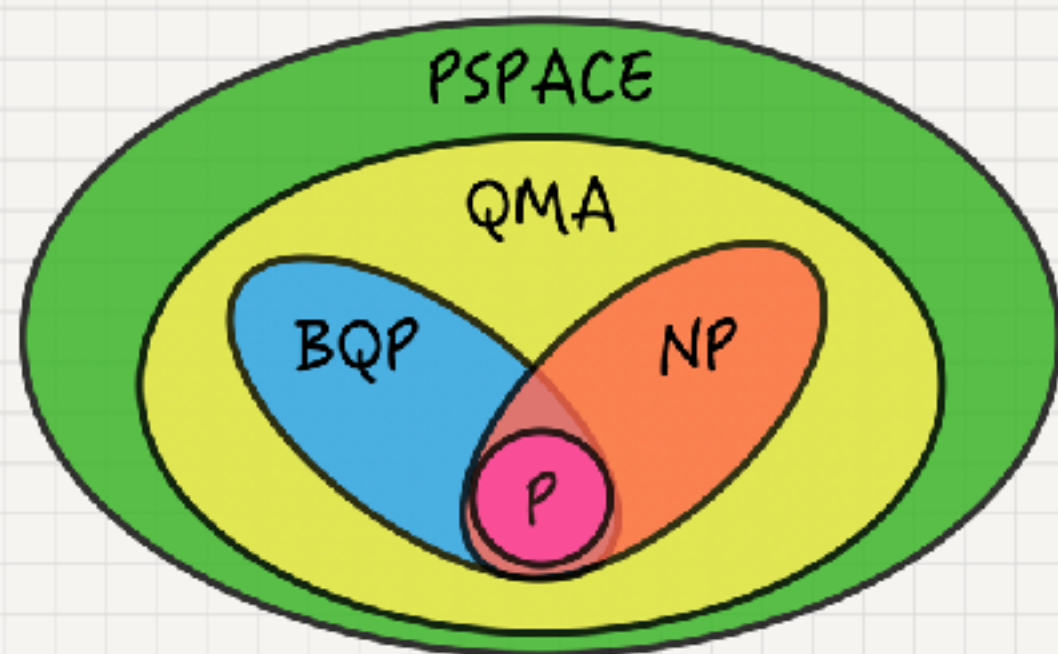


Quantum Complexity Theory

Lecture 3: BQP and QMA

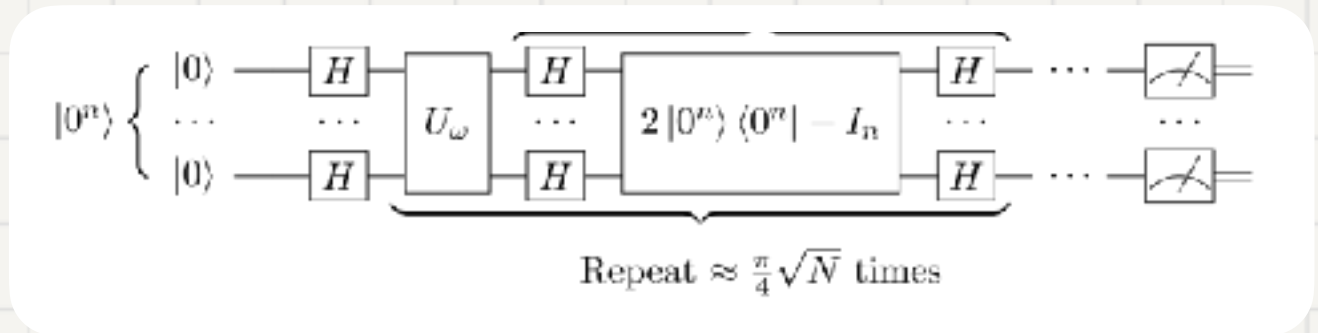
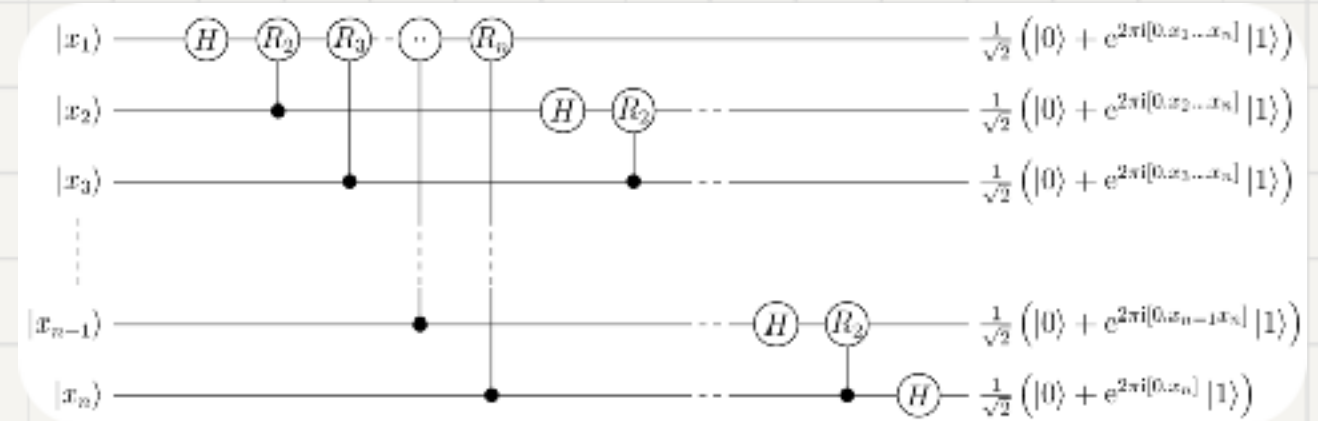
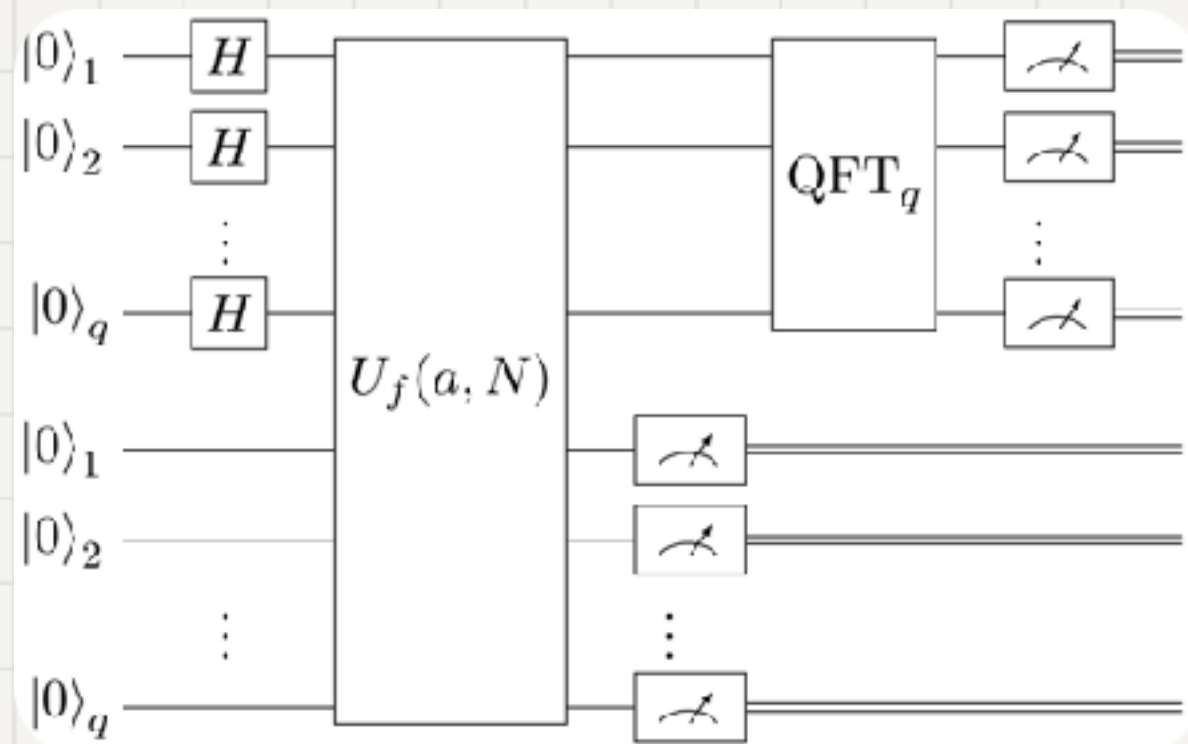


Tom Gur



UNIVERSITY OF
CAMBRIDGE

Quantum algorithms



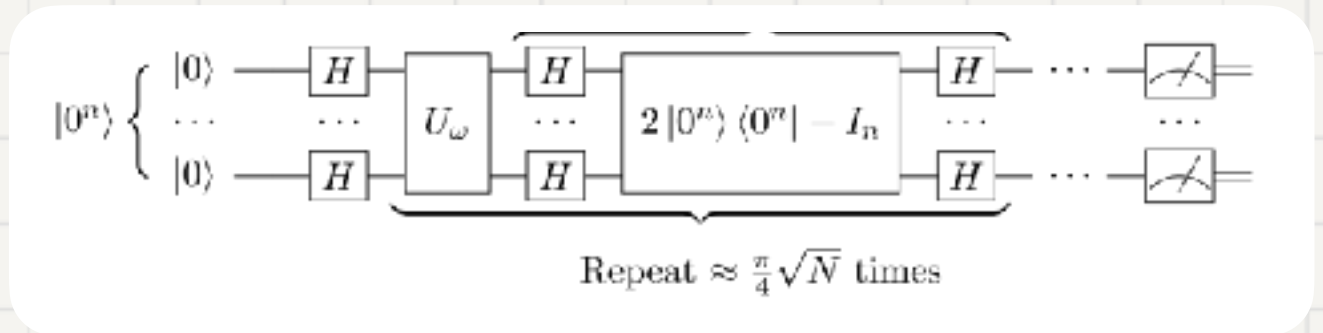
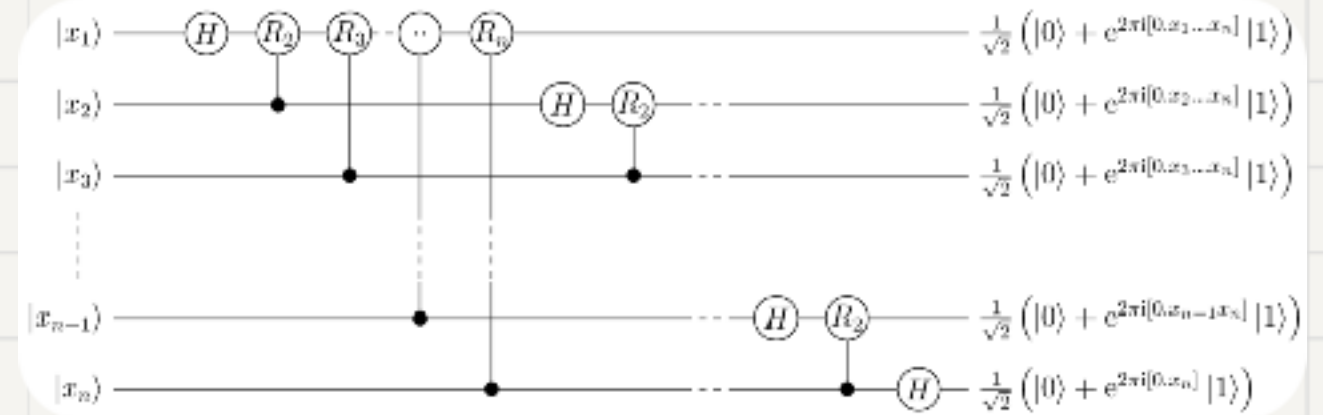
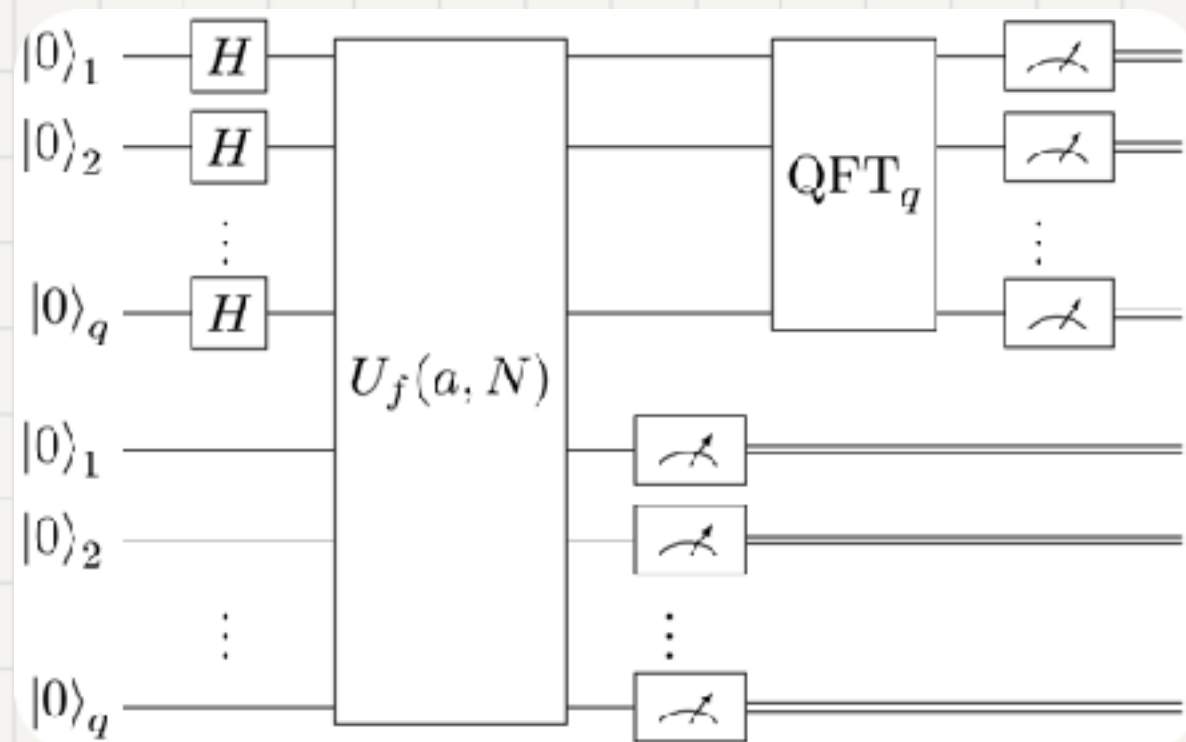
1) Initialize input qubits + ancillas

2) Apply unitary gates

3) Perform a measurement

Why circuits and not
Turing machines?

Quantum algorithms



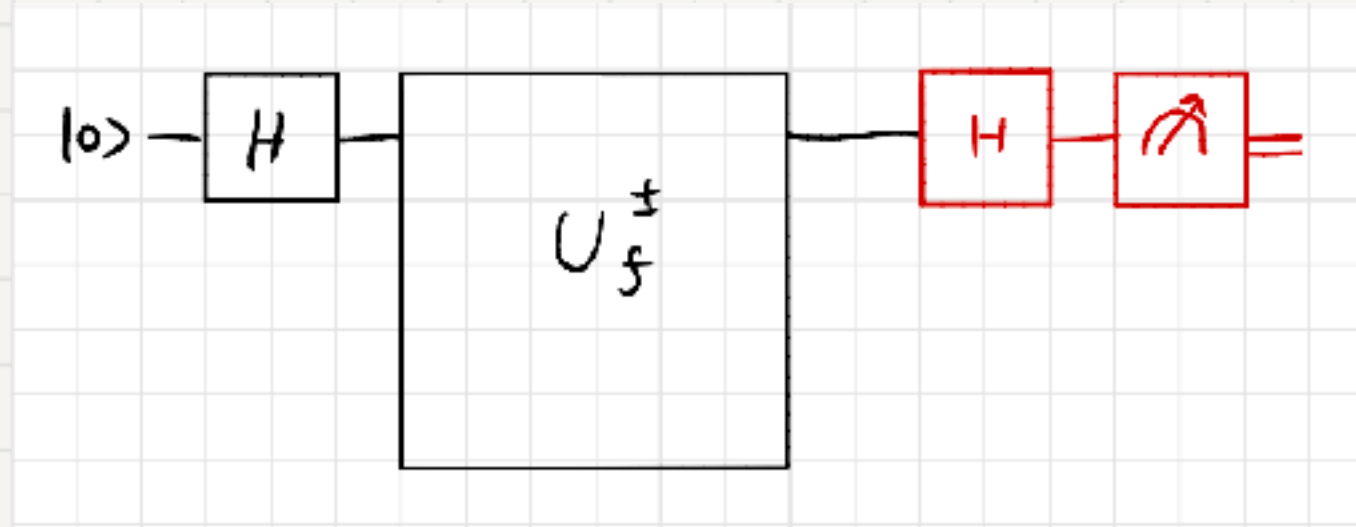
3 examples where quantum algorithms excel:

- ① Finding sub-group structure (Shor's factoring)
- ② Rapid mixing of Markov chains (Grover's search)
- ③ Computing Fourier Transforms (QFT)

Example: quantum algorithm for parity

Goal: Given $f: \{0,1\} \rightarrow \{0,1\}$, compute $f(0) \oplus f(1)$

where f is represented by $U_f^\pm$, mapping $|x\rangle \rightarrow (-1)^{f(x)} |x\rangle$



After Hadamard: $\frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle = |+\rangle$

After query: $\frac{(-1)^{f(0)}}{\sqrt{2}} |0\rangle + \frac{(-1)^{f(1)}}{\sqrt{2}} |1\rangle = \frac{(-1)^{f(0)}}{\sqrt{2}} (|0\rangle + (-1)^{f(1)-f(0)} |1\rangle)$

If $f(0) = f(1)$, we get $|+\rangle$, and after Hadamard $|0\rangle$

If $f(0) \neq f(1)$, we get $|-\rangle$, and after Hadamard $|1\rangle$

Nothing but
Fourier analysis!

Quote of the day

I think I can safely say that nobody understands quantum mechanics
— Richard Feynman



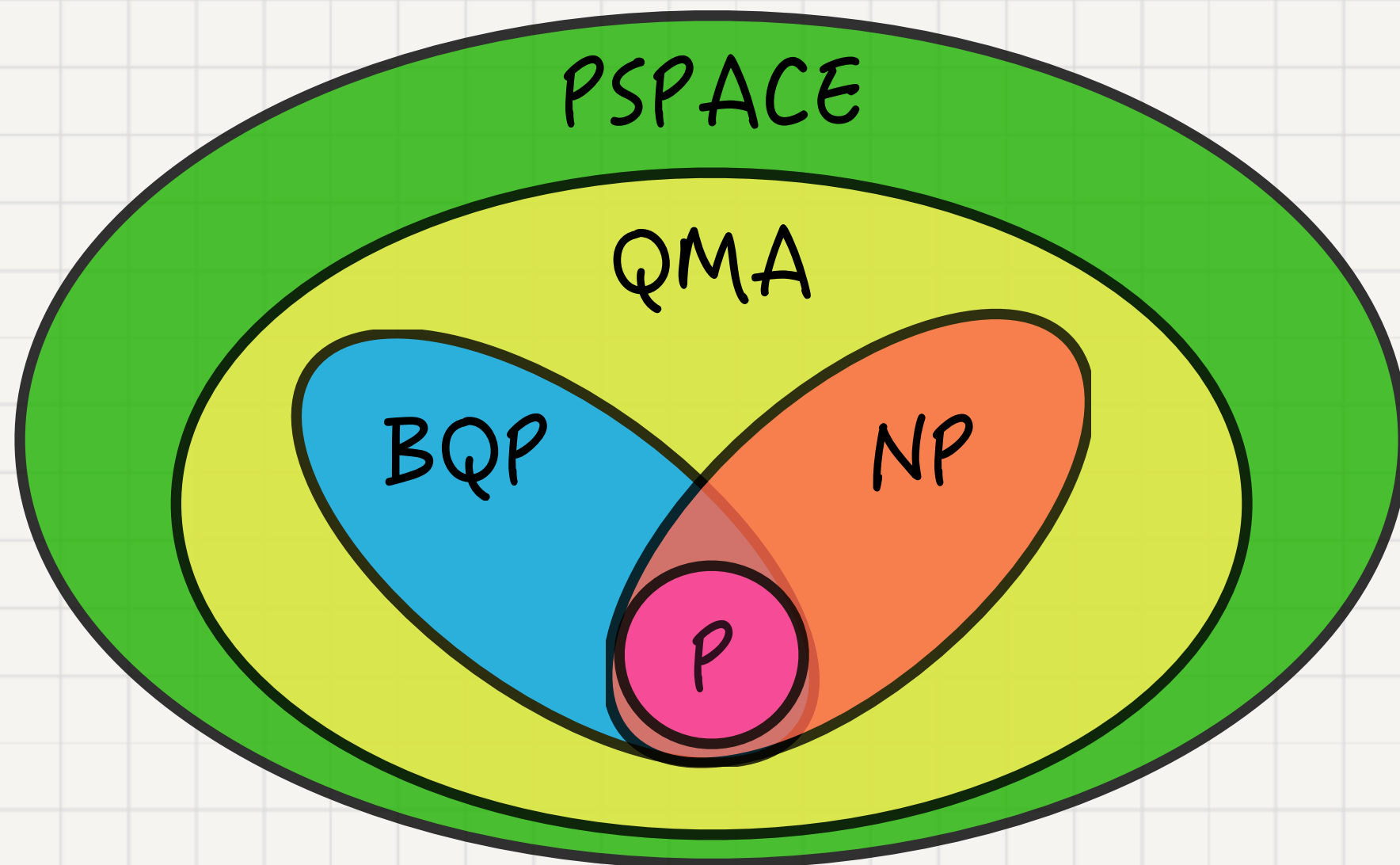
If you think quantum mechanics is weird,
you should try quantum complexity theory

— Scott Aaronson

Quantum complexity classes

BQP = "quantum P"

QMA = "quantum NP"



BQP

The set of all problems solvable by a
poly-time uniform quantum circuits
 $(C_n)_{n \in \mathbb{N}}$ of polynomial size, w.p. $\geq 2/3$
(i.e., $\forall x \in \{0,1\}^n \Pr[C_n(x) = \mathbb{1}_L(x)] \geq 2/3$)

$T(n)$ -uniformity: C_n can be generated
in $T(n)$ time

Circuit size: #gates $\rightarrow$ time complexity

BQP Soundness amplification

Claim 1 (Chernoff bound). Let $A_1, \dots, A_t$ be independent identically distributed random variables taking values in $\{0, 1\}$. Then,

$$\Pr \left[\left| \frac{\sum_i A_i}{t} - \mathbb{E}[A_i] \right| \geq \delta \right] \leq 2e^{-t\delta^2/2}.$$

Let $A_1, \dots, A_t$ be the outputs of invocations of a quantum circuit $C(x)$.

Let $A = \frac{1}{t} \sum_{i=1}^t A_i$ be the average output.

The amplified quantum algorithm C' rules by majority.

On a 1-instance, $\mathbb{E}[A] \geq 2/3$, and the Chernoff bound gives

$$\Pr[|A - 2/3| \geq 1/6] \leq 2e^{-t(1/6)^2/2} = \exp(-t)$$

The analysis for 0-instances is symmetric.

Factoring

Given $n \in \mathbb{N}$, output primes $p_1, \dots, p_n$ s.t.

$$n = p_1 \cdot p_2 \cdot \dots \cdot p_n$$

Decision problem $\text{Factor}(n, k) = 1$

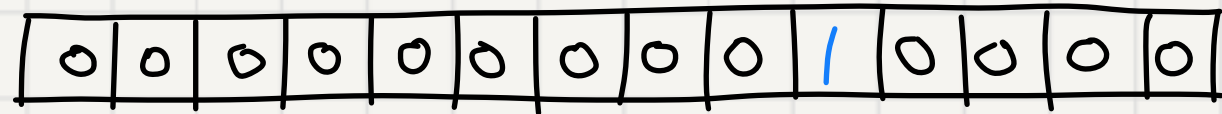
iff n has a prime factor $\leq k$

Shor's algorithm $\text{Factor} \in \text{BQP}$

We know $\text{Factor} \in \text{NP} \cap \text{coNP}$.

Grover's search

Given a string $x \in \{0,1\}^n$, output $i \in [n]$ such that $x_i = 1$



Classical complexity? $\Omega(n)$

Quantum complexity $\Omega(\sqrt{n})$

Quantum Fourier Transform

Given $(f_1, f_2, \dots, f_N) \in \mathbb{C}^N$, output the DFT $(\hat{f}_1, \hat{f}_2, \dots, \hat{f}_N)$

Classical complexity? $O(N \log N)$ Quantum complexity $\tilde{O}(\log N)$

QMA (Quantum NP)

Def $L \in \text{QMA}$ if $\exists$ BQP algorithm V s.t.

$$\forall x \in L \exists |\psi\rangle \text{ s.t. } \Pr[V(|x\rangle|\psi\rangle) = 1] \geq 2/3$$

$$\forall x \notin L \forall |\psi\rangle \Pr[V(|x\rangle|\psi\rangle) = 1] < 1/3$$

For NP we had SAT as a complete problem

$$\phi = (x_1 \vee x_2 \vee x_3) \wedge (x_2 \vee \neg x_1 \vee x_4) \wedge (\neg x_3 \vee \neg x_4 \vee x_5)$$

QMA-complete problem

Def A k -local Hamiltonian is $H = H_1 + \dots + H_m$,

where $\forall_i$ H_i is Hermitian acting on k qubits.

The energy H assigns to $|\psi\rangle$ is $\langle\psi|H|\psi\rangle$.

The ground state minimise the energy $E_G = \min_{|\psi\rangle} \langle\psi|H|\psi\rangle$.

Goal Is $E_G \leq a$ or $E_G \geq b$?

Physical interpretation

Schrodinger's equation $|\psi(t)\rangle = e^{-iHt} |\psi(0)\rangle$

Example of a QMA protocol

Group membership (GM) problem: Group G , subgroup

$H \leq G$ generated by $\{g_1, \dots, g_k\}$. Is $h \in H$?

NP proof: $g_{i_1} \cdot g_{i_1} \cdot \dots \cdot g_{i_n} = h$

Can n be exponential?

Group non-membership (GNM) problem: Group G , subgroup

$H \leq G$ generated by $\{g_1, \dots, g_k\}$. Is $h \notin H$?

Not known to be in NP

What about QMA?

Example of a QMA protocol

Group non-membership (GNM) problem: Group G , subgroup

$H \leq G$ generated by $\{g_1, \dots, g_k\}$. Is $h \notin H$?

QMA proof: $|\pi\rangle = \frac{1}{\sqrt{|H|}} \sum_{g \in H} |g\rangle$

Verifier: w.p. $1/2$ uniformity test, w.p. $1/2$ membership test

1. Sample $b \in H$

