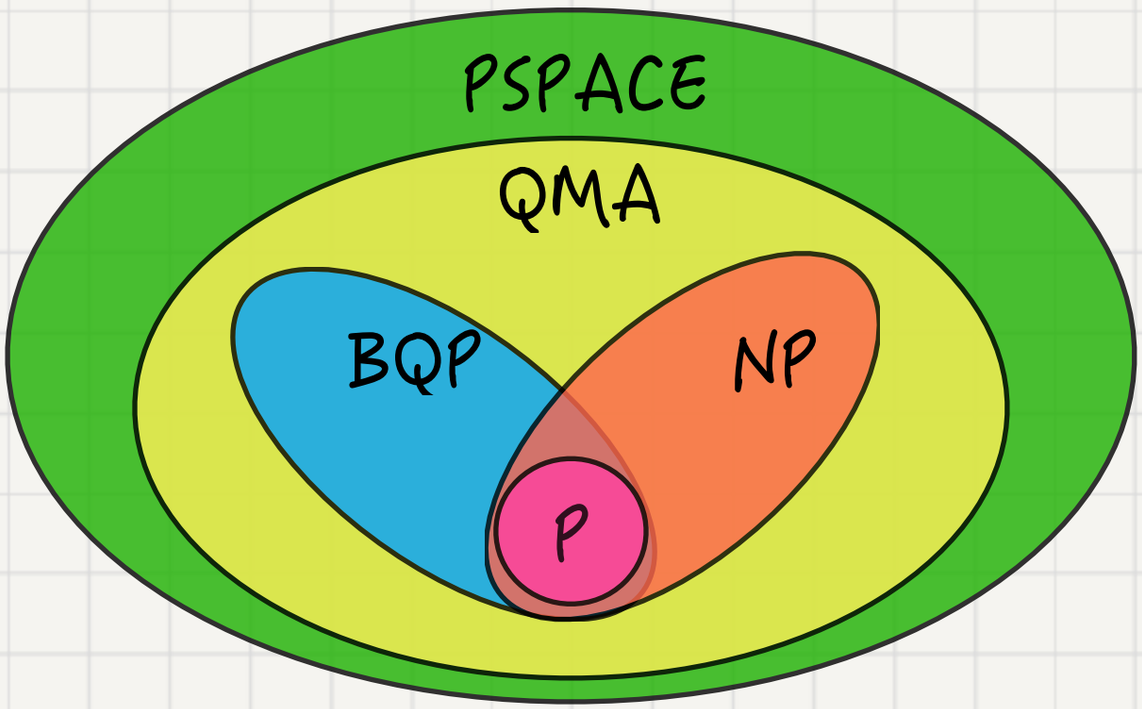
Quantum Complexity Theory

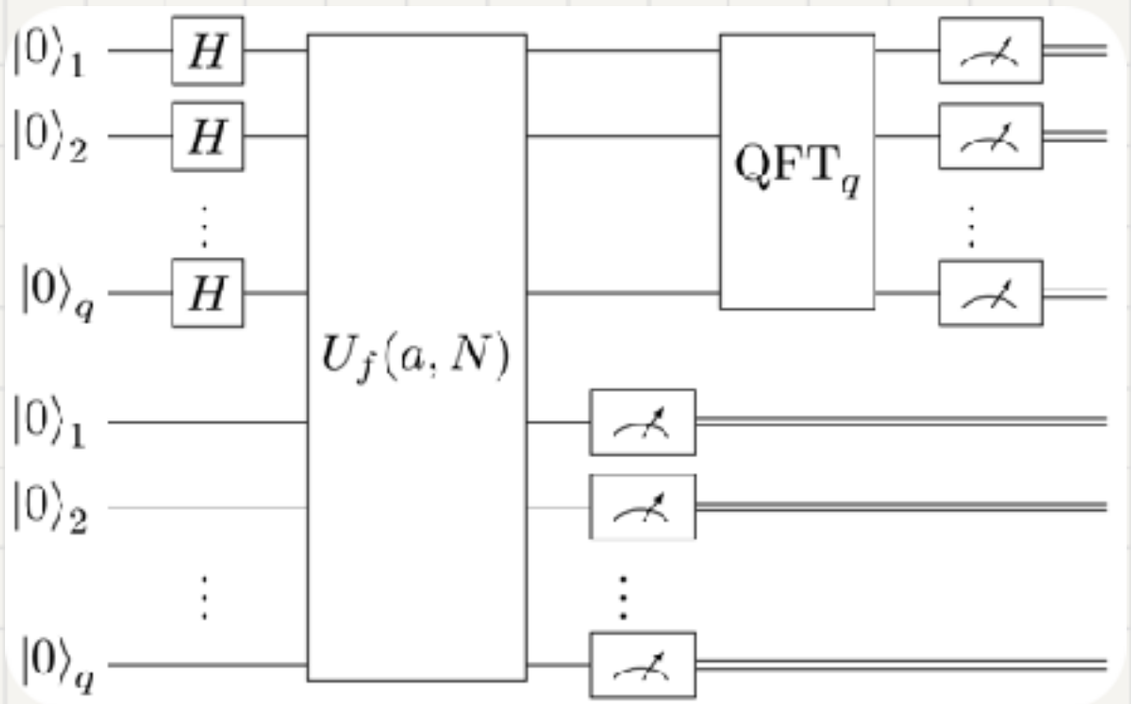
Lecture 4: BQP and QMA

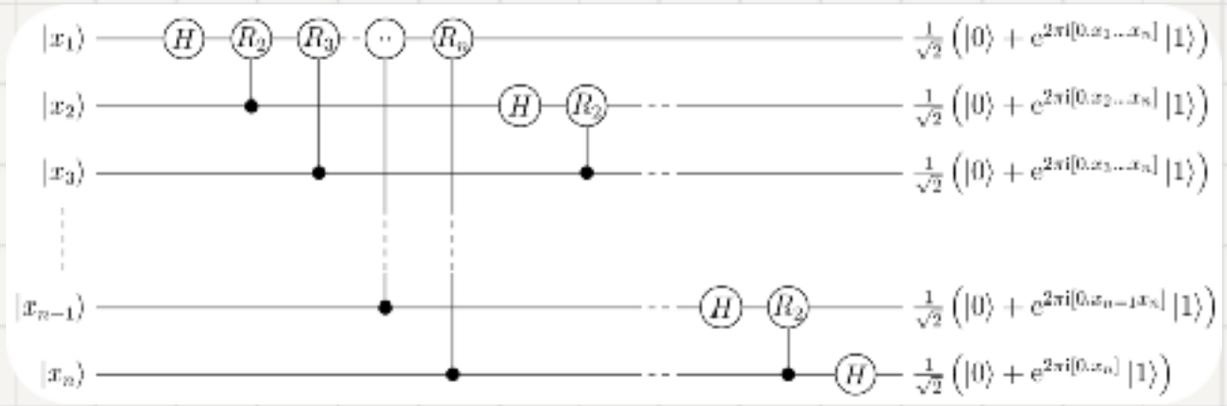


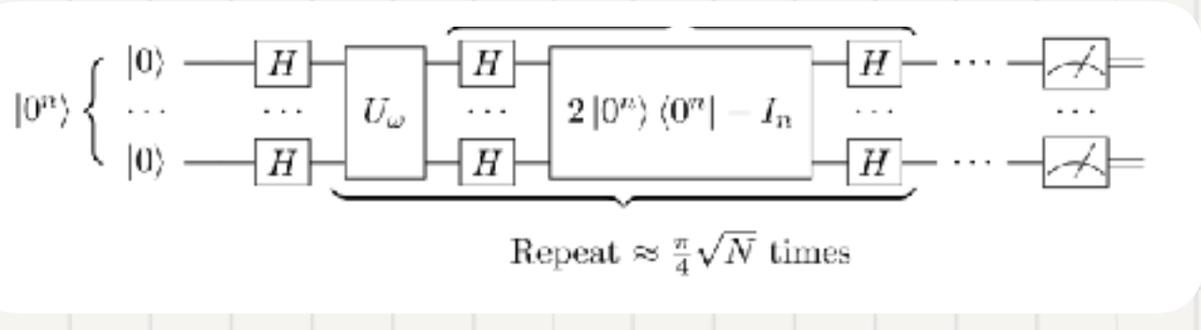
Tom Gur

UNIVERSITY OF CAMBRIDGE

Quantum algorithms







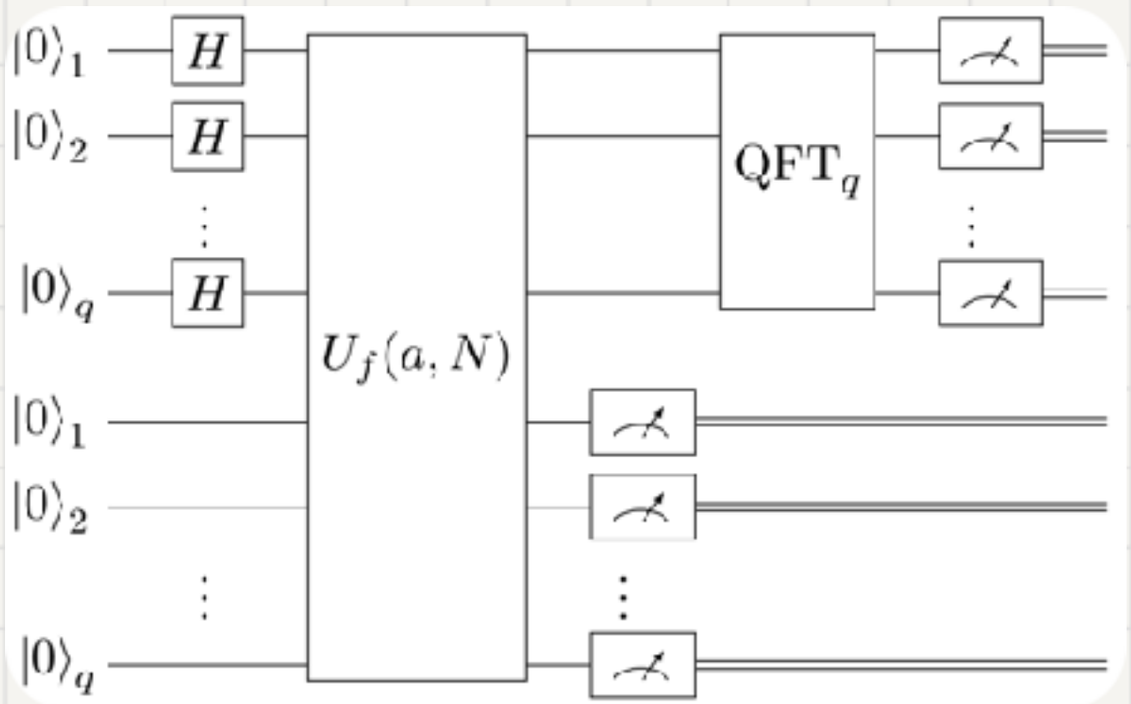
1) Initialize input qubits + ancillas

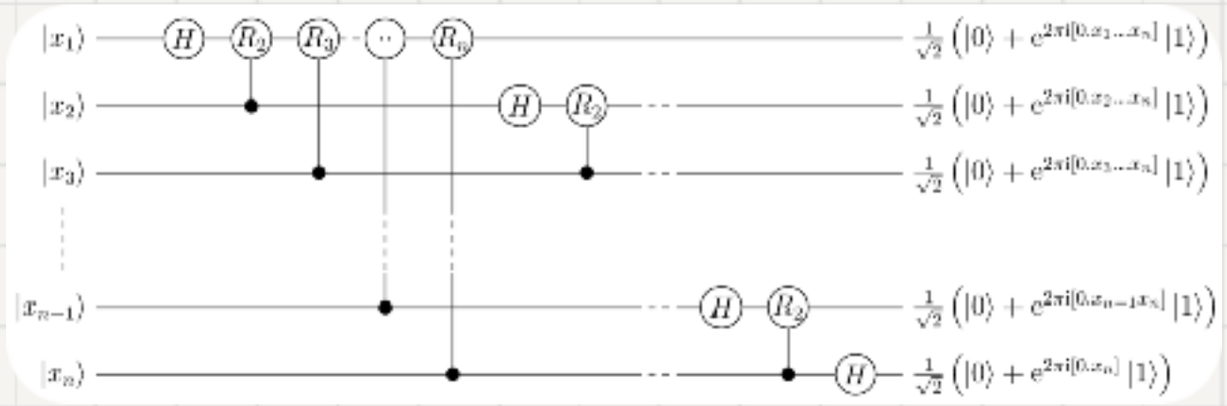
2) Apply unitary gates

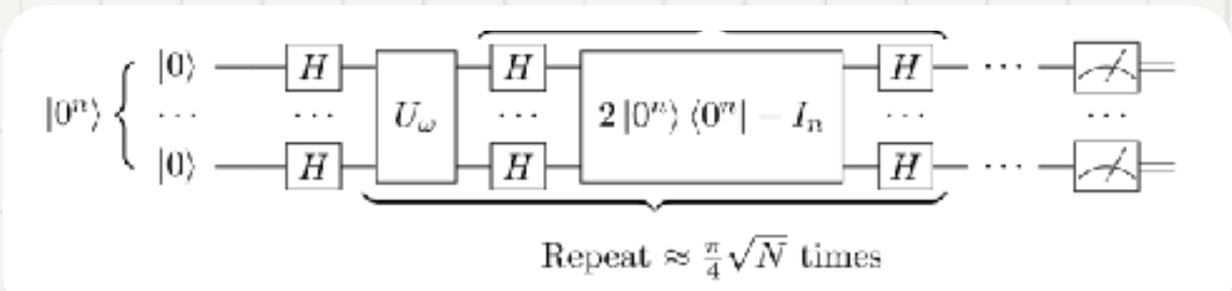
3) Perform a measurement

Why circuits and not Turing machines?

Quantum algorithms







3 examples where quantum algorithms excel:

I Finding sub-group structure (Shor's factoring)

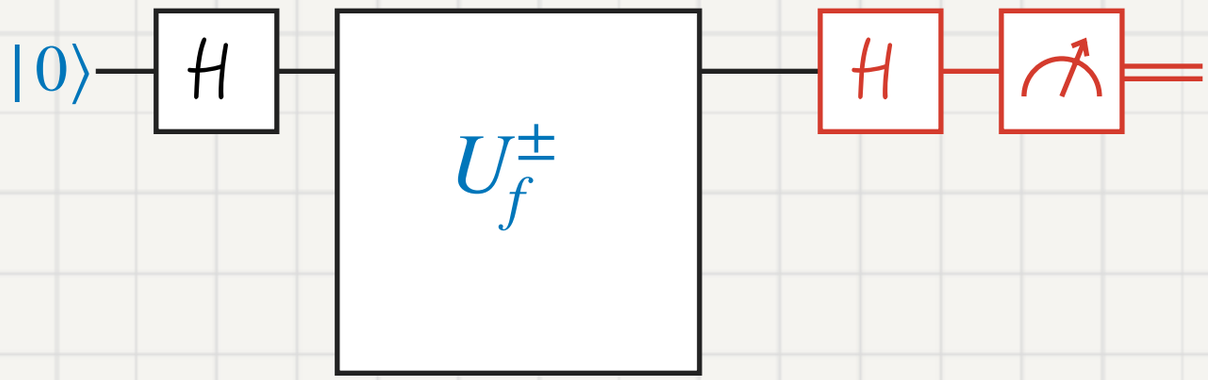
II Rapid mixing of Markov chains (Grover's search)

III Computing Fourier Transforms (QFT)

Example: quantum algorithm for parity

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

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



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

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

If $f(0) = f(1)$, we get $|+\rangle$, and after Hadamard $|0\rangle$ Nothing but

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

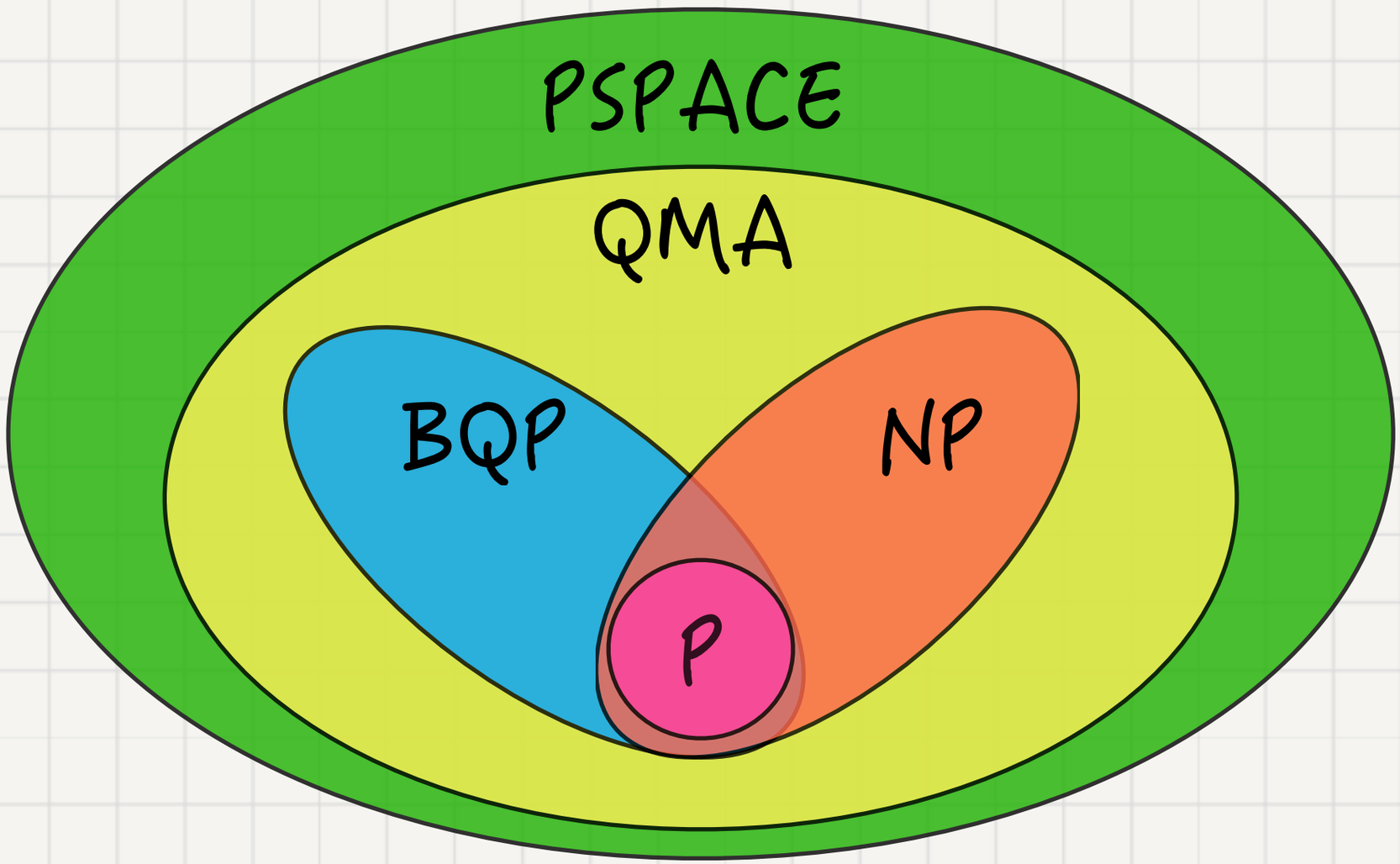
you should try **quantum complexity theory**

— 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., $\forall x \in \{0,1\}^n \quad \Pr[C_n(x) = 1_L(x)] \geq 2/3$)

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

Circuit size: #gates → time complexity

BQP Soundness amplification

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

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

Let $A_1, \ldots, A_t$ 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 $p_1, \cdots, p_n$ s.t.

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

Decision problem

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

iff n has a prime factor $\leq k$

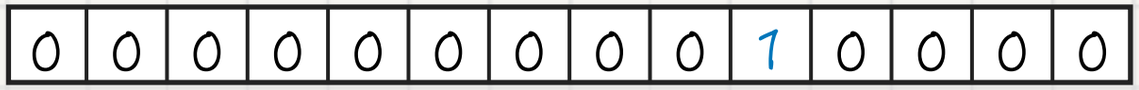
Shor's algorithm

$\text{Factor} \in \text{BQP}$

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

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

What the quantum Fourier transform outputs

An m-qubit register has $N = 2^m$ amplitudes.

$$\sum_{j=0}^{N-1} f_j |j\rangle \longmapsto \sum_{k=0}^{N-1} \hat{f}_k |k\rangle$$

$$\hat{f}_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i j k/N} f_j, \qquad \sum_j |f_j|^2 = 1$$

Exact QFT: $O(m^2)$ gates

Measurement samples a Fourier index. It does not list all coefficients.

Applications extract structure, such as a period or an eigenphase.

QMA (Quantum NP)

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

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

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

The witness contains polynomially many qubits in the input length

For NP we had 3SAT 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 $H = H_1 + \cdots + H_m$,

where $\forall i$ H_i is Hermitian acting on k qubits.

The energy H assign 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

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

Local Hamiltonian: the promise

Polynomially many local terms act on n qubits.

$$H = \sum_{j=1}^{m} H_j, \qquad 0 \le H_j \le I, \qquad b - a \ge \frac{1}{\mathrm{poly}(n)}$$

YES	Outside promise	NO
$E_0 \le a$	$a < E_0 < b$	$E_0 \ge b$

Example of a QMA protocol

Group membership (GM) problem: Group G, subgroup

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

NP proof: $g_{i_1} \cdot g_{i_1} \cdot \ldots \cdot g_{i_n} = h$ Can n be exponential?

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

$H \leq G$ generated by $\{g_1, \ldots, g_k\}$. 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 $\{g_1, \ldots, g_k\}$. 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 $b \in H$
2. 