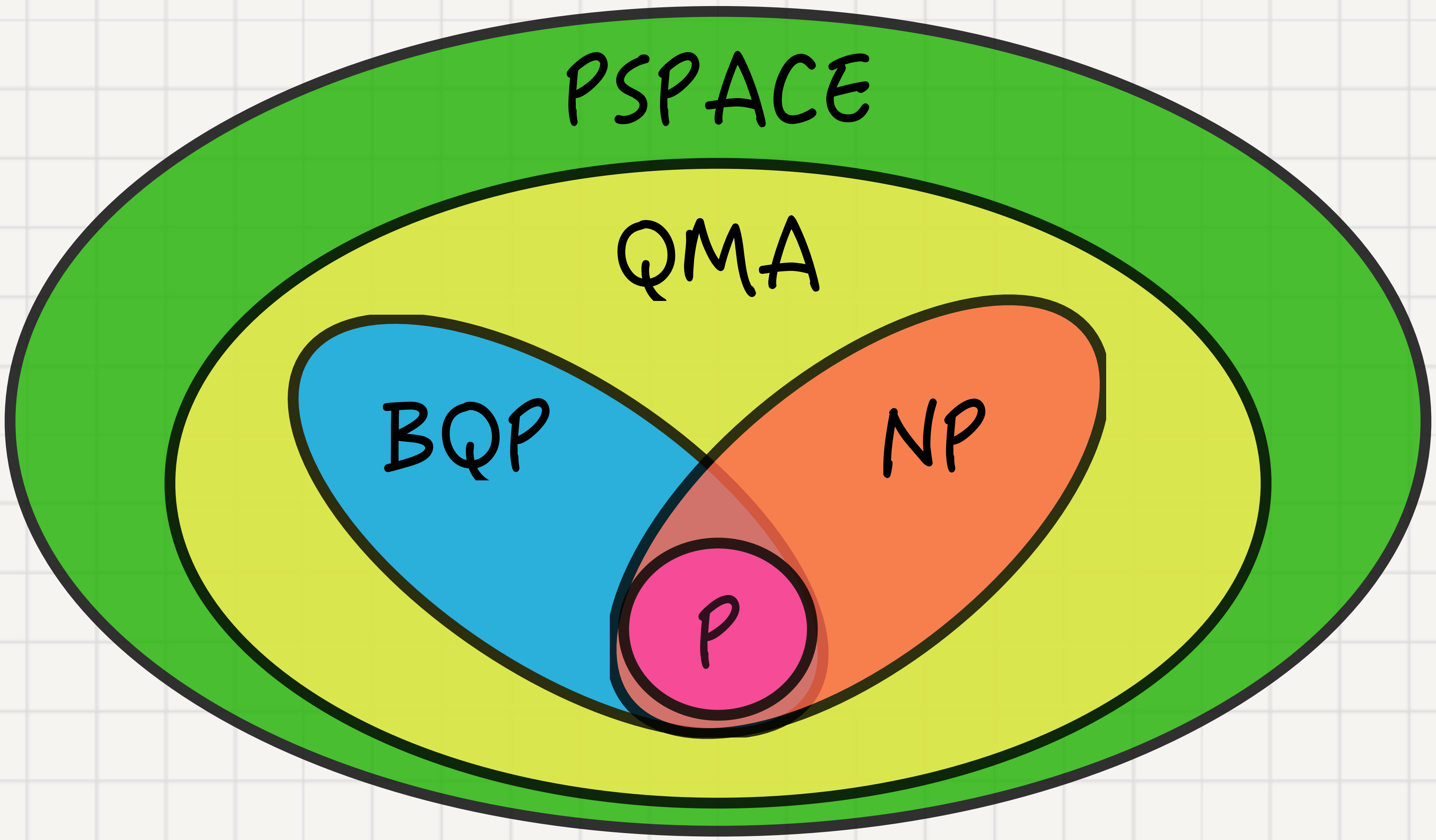
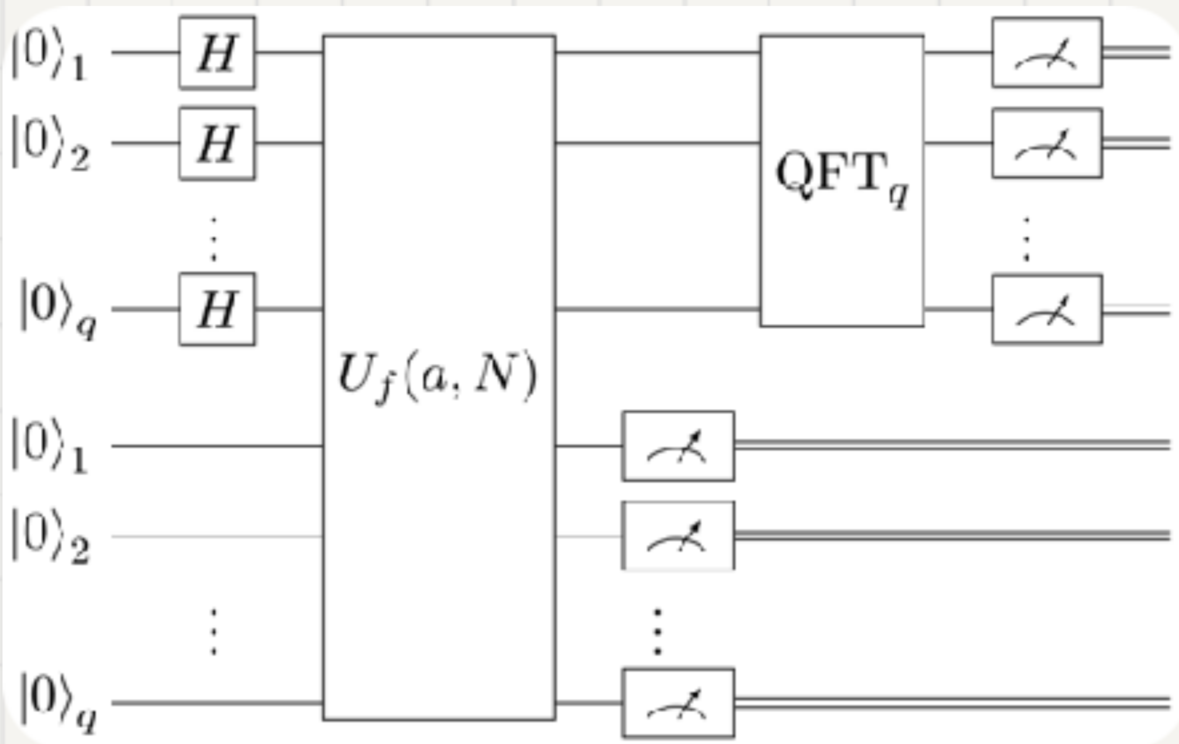
# Quantum Complexity Theory

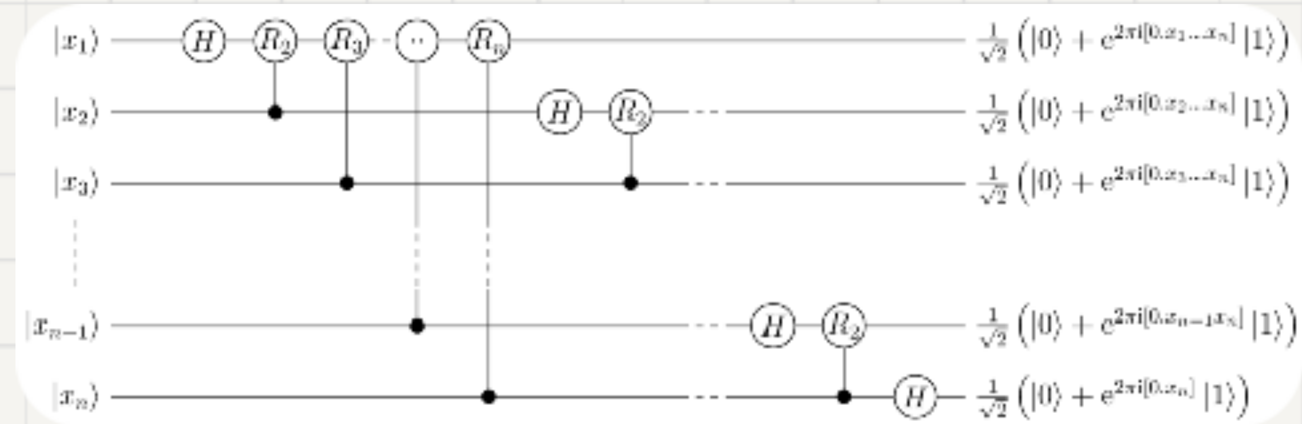
## BQP and QMA complexity classes

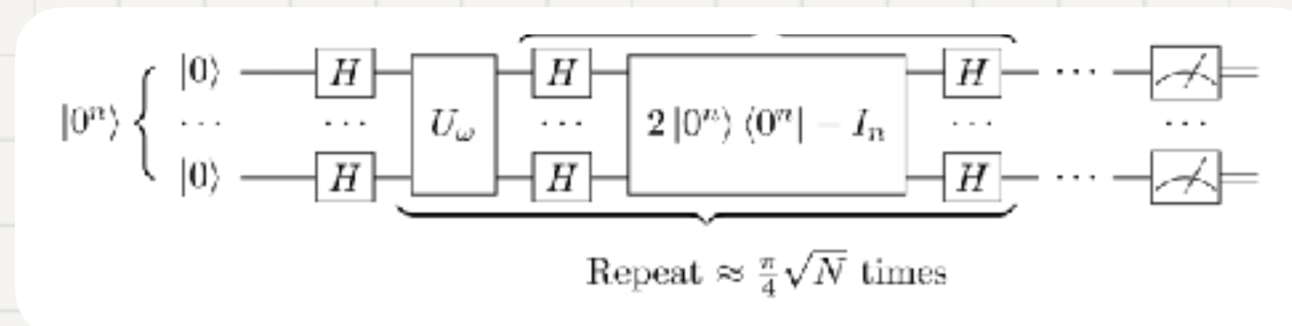



Tom Gur

# Quantum algorithms



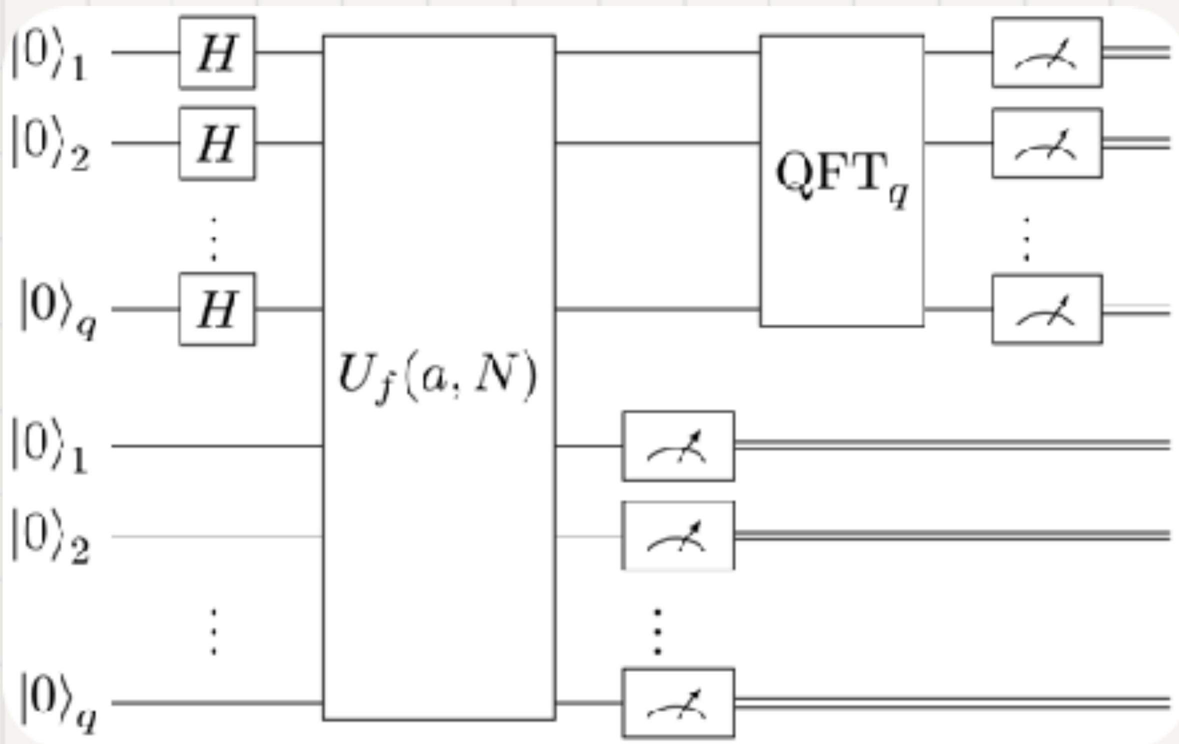

1) Initialize input qubits + ancillas

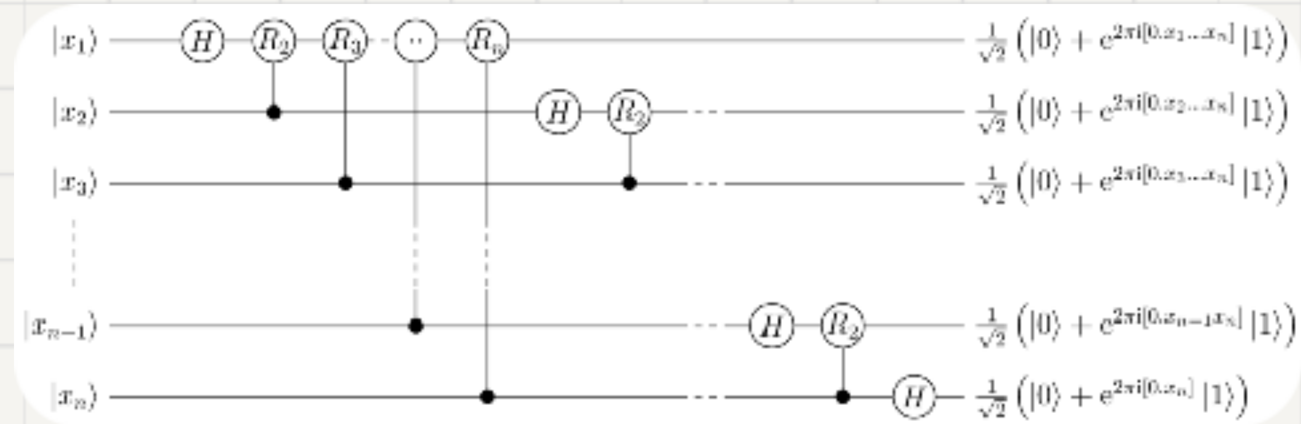
2) Apply unitary gates

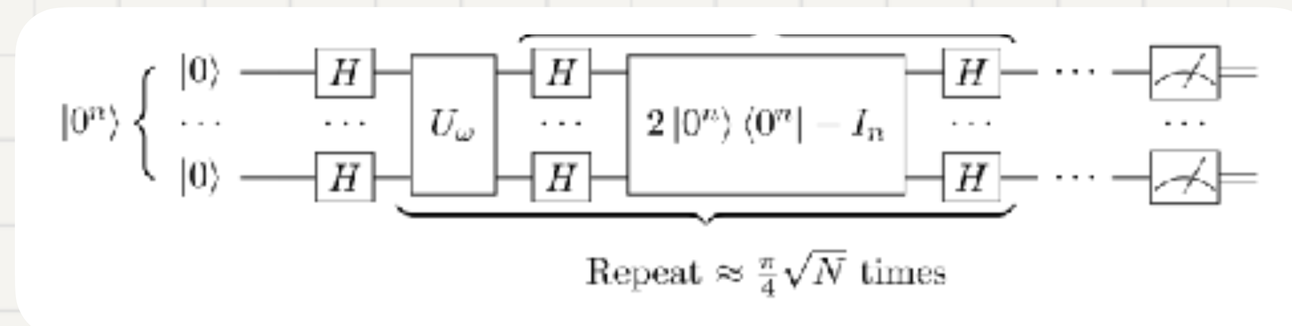
3) Perform a measurement

Why circuits and not Turing machines?

# Quantum algorithms






3 examples where quantum algorithms excel:

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

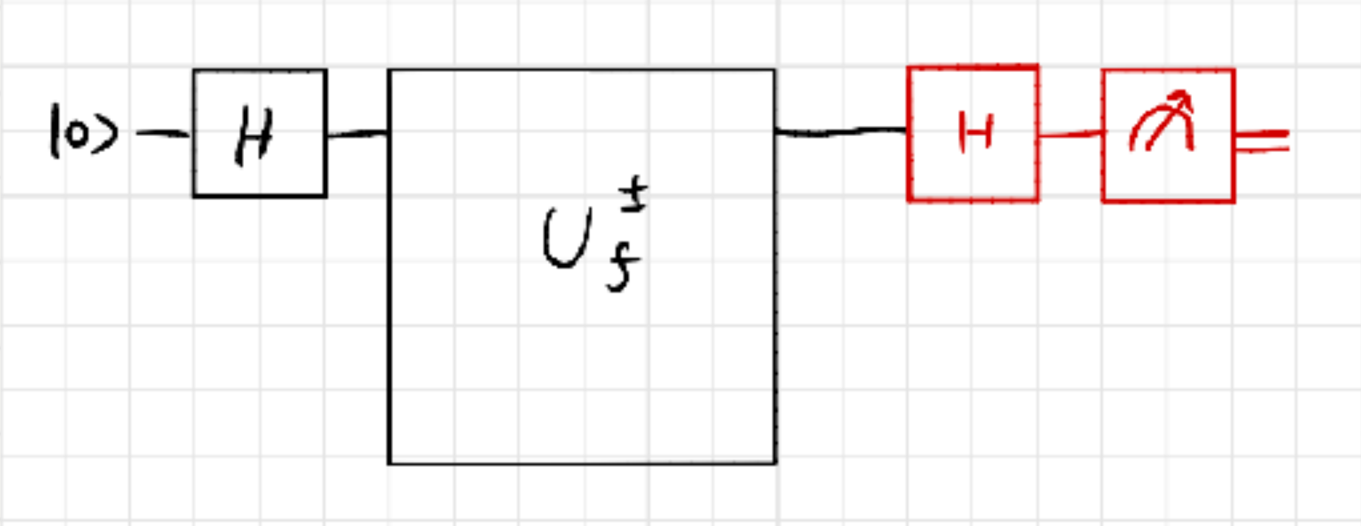
II Rapid mixing of Markov chains (Grover's search)

III Computing Fourier Transforms (QFT)

# Example: quantum algorithm for parity

Goal: Given $f: \{0,1\} \to \{0,1\}$, 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: $\frac{1}{\sqrt{2}} \left( (-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle \right) = \frac{(-1)^{f(0)}}{\sqrt{2}} \left( |0\rangle + (-1)^{f(1)-f(0)} |1\rangle \right)$

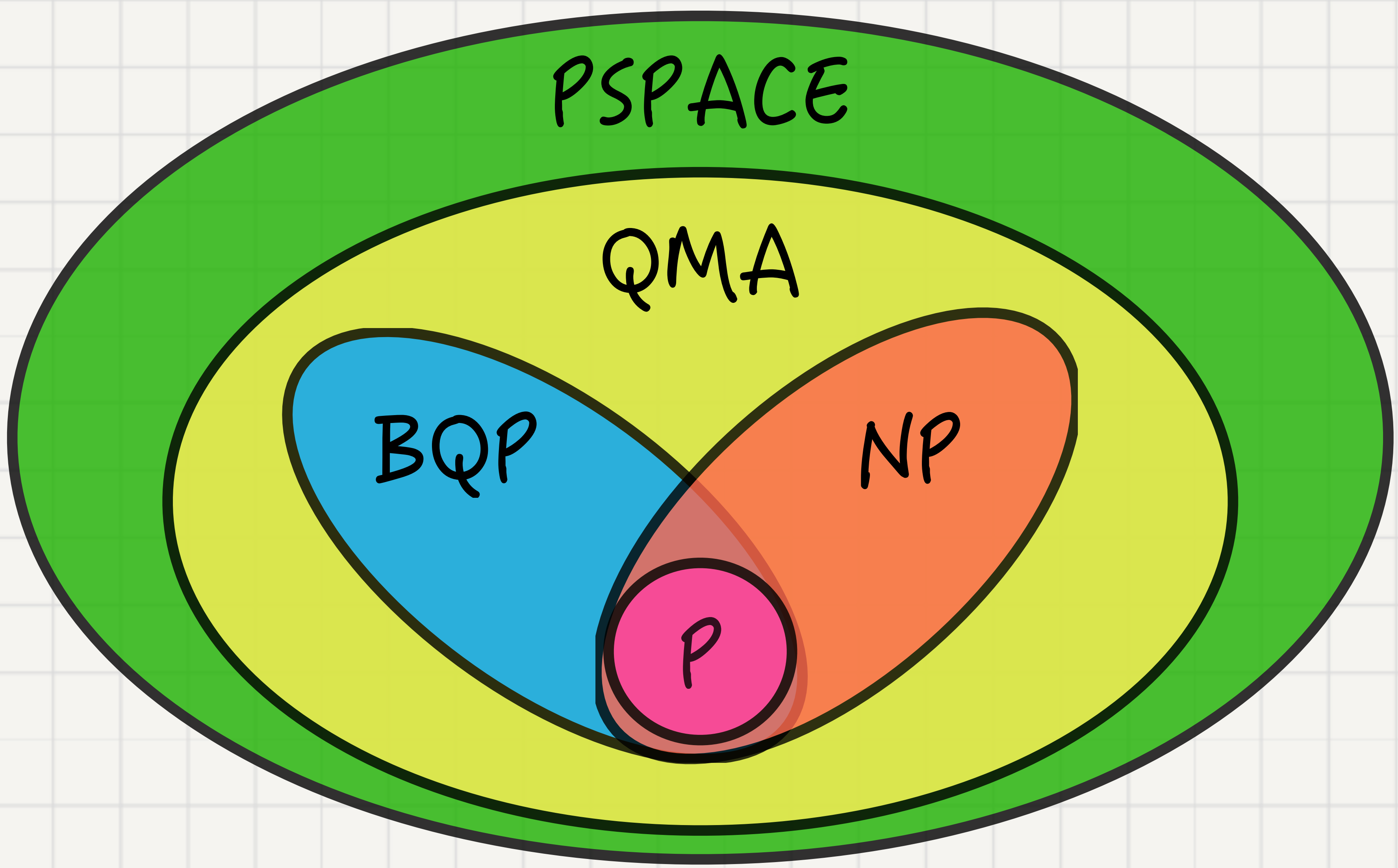
If $f(0) = f(1)$ ,we get $| + \rangle$, and after Hadamard $|0\rangle$

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

# 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 $A_1, \ldots, A_t$ 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 $p_1, \dots, p_n$ 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 $x_i = 1$

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 |

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 $\tilde{O}(\log N)$

# QMA (Quantum NP)

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

$\forall x \in L \ \exists |\psi\rangle$ 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 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 $H = H_1 + \dots + H_m$,

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 $E_G \le a$ or $E_G \ge b$ ?

**Physical interpretation**

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

# Classical-Quantum dictionary (Yuen)

| | |
|---|---|
| SAT | Local Hamiltonian |
| Variables | Qubits |
| constraints/clauses | Hamiltonian terms |
| Assignments | Quantum states |
| # satisfied constraints | Energy |
| Optimal assignment | Ground state |
| Satisfiable | Frustration-free |

# 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