

Complexity Theory

Lecture 12

Quantum Complexity

Mathematical abstraction of quantum computing

Quantum mechanics is an ℓ_2 probability theory

Fully captured by 4 postulates:

① Superposition

A quantum state

is a vector $v \in \mathbb{C}^n$

s.t. $\|v\|_2^2 = 1$.

Ex: a qubit $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$, $\alpha^2 + \beta^2 = 1$

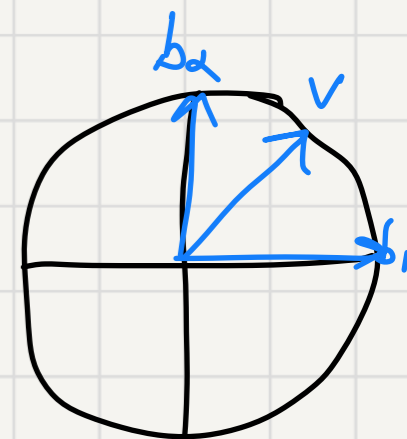
② Measurement

Measuring state $v \in \mathbb{C}^n$ in

orthonormal basis $\{b_1, \dots, b_n\}$

collapses to b_i

w.p. $|\langle v, b_i \rangle|^2$



Mathematical abstraction of quantum computing

III Evolution

A quantum state $v \in \mathbb{C}^n$

evolves to $v' \in \mathbb{C}^n$

via a unitary map

$$\begin{pmatrix} | \\ | \\ v' \\ | \\ | \end{pmatrix} = \begin{pmatrix} U \end{pmatrix} \cdot \begin{pmatrix} | \\ | \\ v \\ | \\ | \end{pmatrix}$$

IV Entanglement

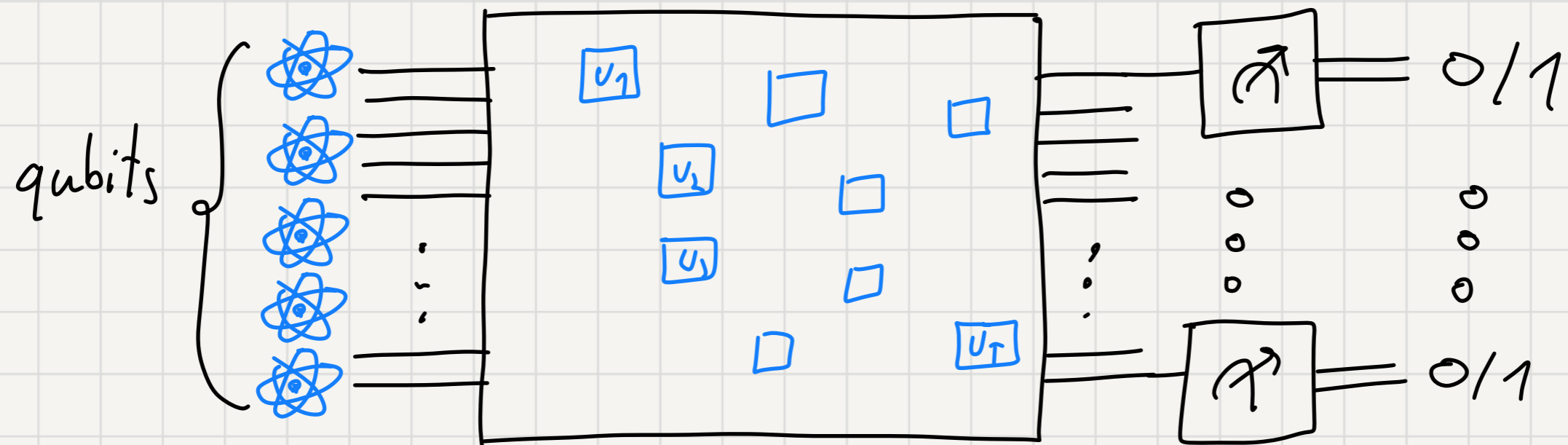
States $u, v \in \mathbb{C}^n$ are

composed via the tensor

product $u \otimes v$.

Ex: $\begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & 000 \\ 0 & 001 \\ 0 & 010 \\ 0 & 011 \\ 0 & 100 \\ 0 & 101 \\ 0 & 110 \\ 0 & 111 \end{pmatrix}$

Quantum algorithms



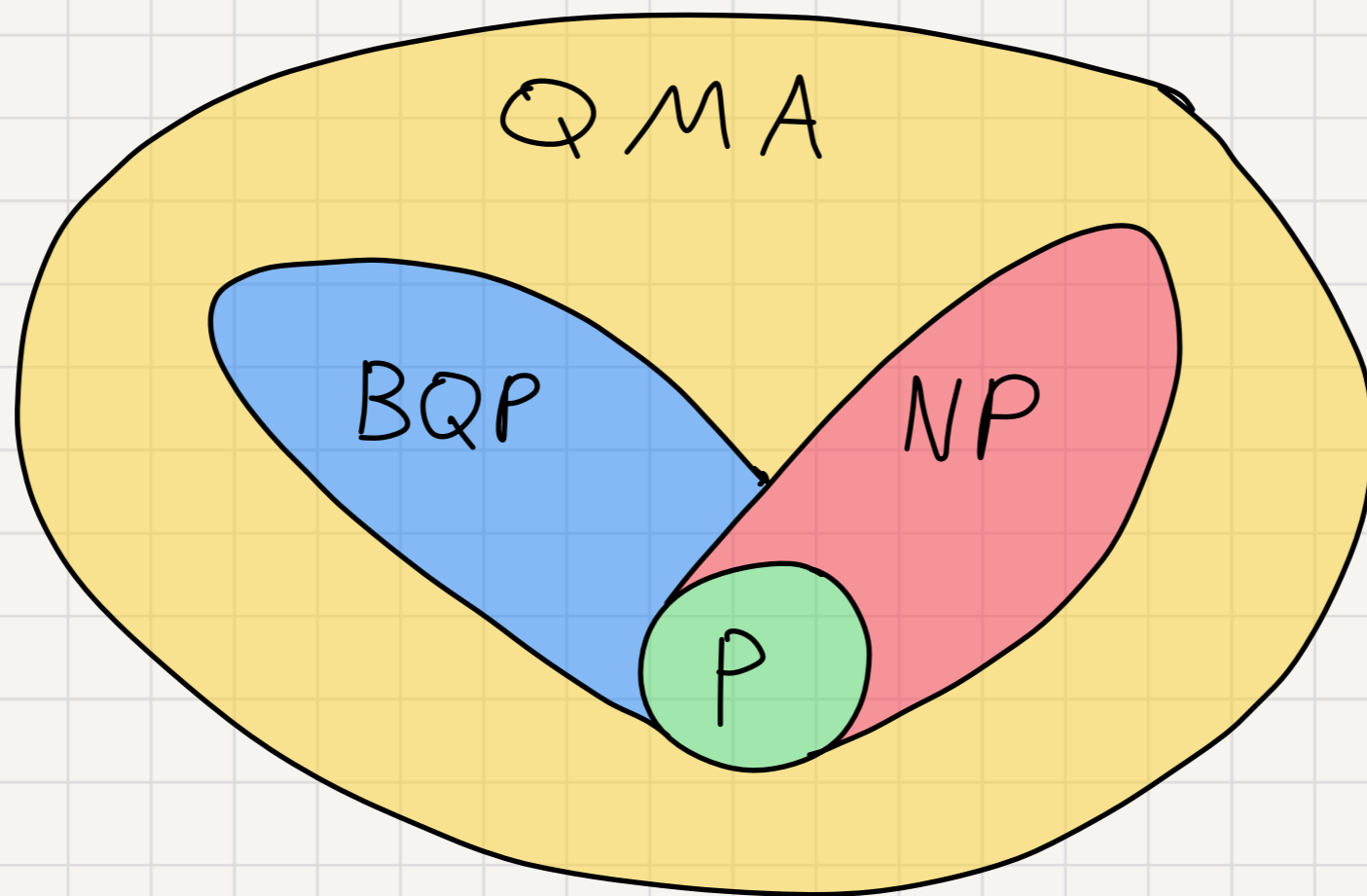
3 examples where quantum algorithms excel:

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

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.

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

Circuit size: #gates

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

Factor $(n, k) = 1$

iff n has a prime factor $\leq k$

Shor's algorithm

Factor $\in \text{BQP}$

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