Quantum Computation

1 Introduction

1.1 Quantum Information Science

Quantum sensing
Quantum cryptography
Quantum networking
Quantum simulation
Quantum computing
Quantum information concepts

1.2 Two Fundamental Ideas

Quantum Complexity:
Quatum error correction

1.3 Strengths

1)Some problems believed to be hard classically, which are easy for quantum computers. Factoring is the best known example,which is useful for cryptigraphy.

2)Complexity theory arguments indicating that quantum computers are hard to simulate classically.

Limitations: we don't believe that quantum computers can efficiently solve worst-case instances of NP-hard optimization problems.

1.4 Why quantum computing is hard

We want qubits to interact strongly with one another.

We don't want qubits to interact with the environment,except when we control or measure them.

Decoherence:Decoherence explains why quantum phenomena, though observable in the microscopic systems studied in the physics lab, are not manifest in the macroscopic physical systems.

To resist decoherence, we must prevent the environment from "learning" about the state of the quantum computer during the computation.

The protected 'logical' quantum information is encoded in a highly entangled state of many physical qubits.

1.5 Quantum computing in the NISQ Era

The (noisy) 50-100 qubit quantum computer has arrived.

Possible quantum examples: Quantum annealers, approximate optimizers, variational eigensolvers, quantum machine learning … playing around may give us new ideas.

NISQ-era quantum devices will not be protected by quantum error correction. Noise will limit the scale of computations that can be executed accurately.

For truly scalable quantum computing, quantum error correction will be required. But QEC has a dauntingly high overhead cost, and will not be feasible in the near term.

Progress toward fault-tolerant QC must continue to be a high priority for quantum technologists.

1.6 Features of Quantum information

Randomness.
Uncertainty.
Entanglement.

1.7 Qubit

Persistent current in a superconducting circuit;
Electron Magnetic Field;
Photon polarization;
Atom Internal State.
$|\psi\rangle = a|0\rangle + b|1\rangle, \quad a, b \in \mathbb{C}, \quad |a|^2 + |b|^2 = 1, \quad |\psi\rangle \sim e^{i\alpha}|\psi\rangle$
A unitary transformation:

$$\begin{aligned} U :& |\varphi\rangle_A \otimes |0\rangle_E \to |\varphi\rangle_A \otimes |e\rangle_E \\ & |\psi\rangle_A \otimes |0\rangle_E \to |\psi\rangle_A \otimes |f\rangle_E \end{aligned}$$

$$(\langle j| \otimes \langle b|)(|i\rangle \otimes |a\rangle) = \delta_{ij}\delta_{ab}.$$

Qubit gates:entangled states(an exponentially large number of two-qubit gates are needed to create the state, starting with a product state.)

1.8 The circuit model

1)Hilbert space of n qubits:

$$|x\rangle = |x_{n-1}\rangle \otimes |x_{n-2}\rangle \otimes \cdots \otimes |x_1\rangle \otimes |x_0\rangle \, , x \in \{0,1\}^n$$

2)Initial state
3)A finite set of fundamental quantum gates.
4) Classical control.
5)Readout.