Concepts and Algorithms of Scientific and Visual Computing

–Advanced Computation Models–

CS448J, Autumn 2015, Stanford University

Dominik L. Michels

Advanced Computation Models

There is a variety of advanced (and sometimes unconventional) computing models including biologically-inspired, chemical, and quantum computing.

We will focus here on quantum computation initially proposed by Richard Feynman in his famous paper

[Feynman 1982]: R. Feynman. Simulating physics with computers.

Later, we will focus on Grover's search, Simon's, and Shor's factorization algorithm.

Please find fundamental and recommendable papers on quantum computing below.

[Bernstein 1993]: E. Bernstein and U. Vazirani. Quantum complexity theory.
[Grover 1996]: L.K. Grover. A fast quantum mechanical algorithm for database search.
[Herbert, 1982]: N. Herbert. FLASH–A superluminal communicator based upon a new kind of quantum measurement.
[Lenstra 1990]: A.K. Lenstra, H.W. Lenstra, Jr., M.S. Manasse, J.M. Pollard. The number field sieve.
[Shor 1994]: P.W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer.
[Simon 1994]: D.R. Simon. On the power of quantum computation.

Copenhagen Interpretation

In 1927 Nils Bohr and Werner K. Heisenberg formulated the

Copenhagen interpretation

of quantum mechanics. According to this interpretation, we do not regard the objects occurring in the quantum theoretical formalism as real. We only use these objects to predict probabilities of measurements.

Similarly, we define the quantum bit as an object describing a superposition of different states.

Quantum Bit

In contrast to a simple bit $b \in \{0,1\}$ used in classical computing, the state of a

$$\text{qubit (quantum bit) } v$$

is given as a superposition of both basis states $|0\rangle$ and $|1\rangle$.

Please note, that we use the Braket-notation here, in which a "Bra" is given by

$$\langle v| = (v_1^*, \ldots, v_n^*)$$

and the "Ket" by

$$|v\rangle = (v_1, \ldots, v_n)^\mathsf{T}.$$

Hence the inner product can be written in the form

$$\langle v, w\rangle = \langle v|(|w\rangle).$$

Quantum Bit

The superposition of both basis states can be expressed by

$$v = \alpha_0 |0\rangle + \alpha_1 |1\rangle$$

with amplitudes α_0, α_1 and $|\alpha_0|^2 + |\alpha_1|^2 = 1$.

Each amplitude is interpreted as the probability, that the qubit is the corresponding state.

The state of the qubit is only a superposition of both states until we perform a measurement. After the measurement, all information about the amplitudes get lost and the qubit is in one of the discrete states $|0\rangle$ and $|1\rangle$.

The state $(|0\rangle + |1\rangle)/\sqrt{2}$ is called uniform. In such cases, we often use implicit normalization and write $|0\rangle + |1\rangle$ instead.

Quantum Bit

As in the classical case, a system of n qubits can be in one of 2^n states. A qubit is given by the superposition of these states.

For example in the case of $n = 2$, we obtain

$$v = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

with

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1.$$

Quantum Entanglement

In contrast to classical bits, because of the so-called

no-cloning theorem

it is not possible to copy the state of a qubit perfectly to another qubit without changing the original qubit.

In [Herbert 1981] the author showed, how it would be possible to send information faster than light by copying qubits. In response to that, [Wootters, Zurek 1982] published the no-cloning theorem.

Unfortunately, according to this, we are not able to use classical error detection and correction methods. On the other hand, it leads to new ways of quantum based algorithms in cryptography.

Quantum Operations

In quantum computing we are able to perform operations, which are allowed by quantum mechanics.

These operations are given by the so-called

Quantum operations

which act on registers of m qubits. Such an operation is given by a function

$$F : \mathbb{C}^{2^m} \to \mathbb{C}^{2^m}$$

whichs maps the actual state to the next state and fulfills the following conditions:

- linearity $\forall_{v \in \mathbb{C}^{2^m}} : F(v) = \sum_x v_x F(|x\rangle)$,
- norm preservation $\forall_{v \text{ with } \|v\|_2 = 1} : \|F(v)\|_2 = 1$.

Quantum Operations

The linearity condition comes from the theory of quantum mechanics and quantum operations have to be norm preserving because only unit vectors are able to describe states.

This conditions are exactly meet by unitary matrices. From this follows, that quantum operations are invertible and compositions of such operations are once again quantum operations.

Because of the linearity, it is sufficient to describe the behavior of quantum operations by the way they operate on the standard basis of $\mathbb{C}^{2^n}$.

Designing a quantum algorithm requires special attention since not every operation from classical computing is unitary.

Quantum Operations

Let us consider some examples for quantum operations:

- flip: a flip of two qubits can be performed by a permutation, which is obviously unitary,
- reorder: can also be performed by a simple permutation,
- rotation: a qubit represented by a 2-dimensional vector can be rotated,
- Hadamard operation: a single qubit operation with the corresponding unitary matrix

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

fulfills $H^2 = \mathbf{1}$.

Quantum Computing

A quantum operation is called a

quantum gate,

if it acts on three or less qubits of a register of m qubits.

A sequence of such operations performed by the application of quantum gate is called

quantum computing

or quantum computation.

Quantum Computing

Let $f : \{0,1\}^* \to \{0,1\}$ and $T : \mathbb{N} \to \mathbb{N}$ be arbitrary functions. We call f

computable in quantum $T(n)$-time,

if there is a classical Turing machine that maps a given input $(1^n, 1^{T(n)})$ for $n \in \mathbb{N}$ to the descriptions of the quantum gates $F_1, \ldots, F_T$ such that for every $x \in \{0,1\}^n$, we can compute $f(x)$ by the following process with a probability of at least $2/3$.

1. Initialize a m-qubit quantum register to the state x padded with zeros $|x0^{n-m}\rangle$, $m \leq T(n)$.
2. Perform a sequential application of the other $T(n)$ quantum gates $F_1, \ldots F_T$ to the register.
3. Measure the register and let Y denote the obtained value. If v is the final state of the register, then Y is a random variable that takes the value y with a probability of $|v_y|^2$ for each $y \in \{0,1\}^m$. After that return Y_1.

Quantum Computing

The class

BQP (bounded error quantum polynomial time)

contains the decision problems solvable by quantum computing in polynomial time with a bounded error probability.

A Boolean function $f : \{0,1\}^* \to \{0,1\}$ is in BQP, if there exists a polynomial function $P : \mathbb{N} \to \mathbb{N}$ such that f is computable in quantum $p(n)$-time.

In the next lecture we will consider the following three quantum algorithms:

- Grover's Search Algorithm,
- Simon's Algorithm,
- Shor's Factorization Algorithm.