QUANTUM COMPUTING

Jozef Gruska
Faculty of informatics, Masaryk university
Botanická 68a, 60200 Brno, Czech Republik[1]

1 Introduction

Quantum computing deals with laws, limitations, phenomena and processes concerning computation in particular, and information processing in general, in case quantum objects are carriers of information. Therefore, the laws, limitations, resources and processes of the quantum world are the ones that have to be used to design quantum information processing systems and have to be applied to explore their potentials and limitations. All that developed an understanding that *information is physical*.

The difference between classical and quantum computers (information processing systems) is therefore in a way information is stored, transferred and processed. In classical computers, information is represented on a *macroscopic level* by *bits*, which can take one of two values 0 or 1. In *quantum computers*, information is represented on a *microscopic level*, using so-called *qubits* (quantum bits), which can take on any from uncountable many superpositions $\alpha|0\rangle + \beta|1\rangle$, where α, β are arbitrary complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$, and $|0\rangle$, $|1\rangle$, so-called ket-vectors, can be seen as the representations of classical bit values 0 and 1.

The existence of quantum states, which can be seen as a superposition of classical states (and in some important cases exponentially large superpositions can be created, as it will be shown later, using a linear amount of physical resources), allows to create massive parallelism. This fact, together with the existence of very special, and inherently quantum, resources, such as quantum entanglement and non-locality,

[1]Support of the grants GACR 201/07/0603 and MSM0021622419 is to be acknowledged.

full of mysteries, allows to create (quantum) information processing systems much outperforming corresponding classical systems.

Design of (quantum) information processing systems of a new quality is one of the goals of the research in the area of quantum information processing and communication (QIPC). This is often seen as the main way to make sure that the Moore law, concerning the development of information processing systems, will still hold for quite a while. The second goal of the research in QIPC, and perhaps even more important one, is to get new insights into the quantum world, reflecting a new emerging view that quantum physics has information as its primary fundamental ingredient, what is then reflected in the slogan*Physics is informational*. In the experimental area, another level of importance of the QIPC research and development is connected with the fact that in many areas of science and technology one increasingly needs expertise with storing, transmission and manipulation of particles.

The history of QIPC goes back to 1982 when Feynman envisioned that new type of computers will be needed to simulate quantum physics. Apt killers for the field were Shor's quantum algorithms that would allow to break some important cryptosystems.

For more details about quantum computing see books [1,2]. For more about underlying theory of computing and quantum physics see the Reading list.

1.1 Hilbert space basics

The physical concept of a quantum system corresponds very well, from the computation point of view, to the mathematical concept of the Hilbert space. Both infinite-dimensional and finite-dimensional Hilbert spaces are of importance for QIPC. For quantum computation, finite-dimensional Hilbert spaces, to be discussed next, are of the main importance.

A Hilbert space $\mathcal{H}_n$ is an n-dimensional complex vector space with

$$\text{an } \textit{inner product } \langle\psi|\phi\rangle = \sum_{i=1}^{n} \phi_i \psi_i^* \text{ of vectors } |\phi\rangle = \begin{vmatrix} \phi_1 \\ \phi_2 \\ \vdots \\ \phi_n \end{vmatrix}, |\psi\rangle = \begin{vmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_n \end{vmatrix},$$

that can be used to define the *norm of a vector* $||\phi|| = \sqrt{|\langle\phi|\phi\rangle|}$ and *metrics* $\mathrm{dist}(\phi,\psi) = ||\phi-\psi||$. This allows to introduce on $\mathcal{H}_n$ such concepts as continuity.

Elements (vectors) of a Hilbert space $\mathcal{H}_n$ of the norm one are usually called n-dimensional *pure states*, or, more physically, n-level systems. Elements of $\mathcal{H}_2$ are called *qubits*. They can be represented by points on a unit sphere, called the *Bloch sphere*. This representation is based on the fact that a general form of a qubit is $\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$ where (θ,ϕ) are seen as *spherical coordinates* of the corresponding point on the Bloch sphere.

Two quantum states $|\phi\rangle$ and $|\psi\rangle$ are called *orthogonal* if their inner product is zero, that is if $\langle\phi|\psi\rangle = 0$.

In every Hilbert space there are so-called *orthonormal bases* - bases all states of which are mutually orthogonal and of the norm one. In the following only orthonormal bases will be considered.

Dirac introduced a handy, so-called bra-ket, notation, to deal with probability amplitudes, quantum states and linear functionals $f : H \to \mathbf{C}$ on any Hilbert space $\mathcal{H}$. If $\psi, \phi \in \mathcal{H}$, then

$\langle\psi|\phi\rangle$ — *inner (scalar or Hermitian) product* of ψ and ϕ — is the *probability amplitude* of a transfer from the state ϕ to ψ;

$|\phi\rangle$ — *ket-vector* ϕ — is an equivalent to ϕ

$\langle\psi|$ — *bra-vector* ϕ — is a linear functional on H such that $\langle\psi|(|\phi\rangle) = \langle\psi|\phi\rangle$;

$|\psi\rangle\langle\phi|$ — *outer product* of $|\psi\rangle$ and $\langle\phi|$ — is a matrix.

Example: For states $\phi = (\phi_1, \dots, \phi_n)$ and $\psi = (\psi_1, \dots, \psi_n)$ we have

$$|\phi\rangle = \begin{pmatrix} \phi_1 \\ \dots \\ \phi_n \end{pmatrix}, \langle\phi| = (\phi_1^*, \dots, \phi_n^*); \langle\phi|\psi\rangle = \sum_{i=1}^{n} \phi_i^* \psi_i; |\phi\rangle\langle\psi| = \begin{pmatrix} \phi_1\psi_1^* & \dots & \phi_1\psi_n^* \\ \vdots & \ddots & \vdots \\ \phi_n\psi_1^* & \dots & \phi_n\psi_n^* \end{pmatrix}$$

It is natural to see an evolution step of a quantum system as a transition from one state to another. Such transitions have to satisfy three principles:

P1 To each transfer from a quantum state ϕ to a state ψ, a complex number $\langle\psi|\phi\rangle$ is associated, called the *probability amplitude* of the transfer, such that $|\langle\psi|\phi\rangle|^2$ is the *probability* of the transfer.

P2 If a transfer from a quantum state ϕ to a quantum state ψ can be decomposed into two subsequent transfers, $\psi \leftarrow \phi' \leftarrow \phi$, then the resulting amplitude of the transfer is the *product* of the amplitudes of the sub-transfers: $\langle\psi|\phi\rangle = \langle\psi|\phi'\rangle\langle\phi'|\phi\rangle$

P3 If a transfer from a state ϕ to a state ψ has two independent alternatives, with amplitudes α and β, then the resulting amplitude is the sum $\alpha + \beta$ of the amplitudes of two sub-transfers (and therefore $\alpha + \beta = 0$ if $\alpha = -\beta$).

In general, an evolution of a quantum system that is in the state $\psi(t)$ in time t is described by the *Schrödinger linear equation*

$$i\hbar\frac{\partial\psi(t)}{\partial t} = H(t)\psi(t),$$

where $H(t)$ is a quantum analogue of a Hamiltonian (in time t) of a classical system, and $\hbar$ is the *Planck constant.* From that it follows that the evolution (computation) of a quantum system is performed by a *unitary operator* $U = e^{iH}$ (for the case Hamiltonian H is constant in time), and a step of such an evolution, when considered in the discrete time, can then be seen as a multiplication of a *unitary matrix*[2] A with a vector $|\psi\rangle$, i.e. as $A|\psi\rangle$.

In case an orthonormal basis $\{\beta_i\}_{i=1}^n$ is chosen in $\mathcal{H}_n$, any state $|\phi\rangle \in \mathcal{H}_n$ can be uniquely expressed in the form

$$|\phi\rangle = \sum_{i=1}^{n} a_i|\beta_i\rangle, \quad \text{where} \quad \sum_{i=1}^{n} |a_i|^2 = 1,$$

$a_i = \langle\beta_i|\phi\rangle$ and $|a_i|^2$ are *probabilities* that if the state $|\phi\rangle$ is measured with respect to the basis $\{\beta_i\}_{i=1}^n$, then the state $|\phi\rangle$ collapses into the state $|\beta_i\rangle$. The classical "outcome" of such a measurement of the state $|\phi\rangle$, with respect to the basis $\{\beta_i\}_{i=1}^n$, is then the index i of that state $|\beta_i\rangle$ into which the state $|\phi\rangle$ collapses.

A more general way to define a quantum (projective) measurement is through observables - Hermitian matrices. Each such matrix A can be decomposed, in a unique way, in the form $A = \sum_{i=1}^k \lambda_i P_i$, where λ_i are different eigenvalues of A and P_i are projectors (projection operators[3]) into the subspaces of eigenvectors corresponding to eigenvalues λ_i. The result of such a measurement is then a (random) projection to one of such subspaces. One can see projective measurement defined by a Hermitian operator as a measurement with respect to the orthonormal basis created by eigenvectors of A.

As a consequence of the peculiarities of quantum measurements, one can "store" safely in a quantum state of $\mathcal{H}_n$ only n bits - that is to store bits in such a way that each of them can be obtained back for sure - this is so-called *Holevo theorem.*

Another important concept, very specific indeed in the quantum case, is that of a composed quantum system. In case a quantum system S_1 (S_2) is represented by a Hilbert space $\mathcal{H}_n$ ($\mathcal{H}_m$), with an orthogonal basis $\{\alpha_i\}_{i=1}^n$ ($\{\beta_j\}_{j=1}^m$), then the *composed quantum system of* S_1 *and* S_2 is represented by the Hilbert space $\mathcal{H}_{nm} = \mathcal{H}_n \otimes \mathcal{H}_m$, the tensor product of $\mathcal{H}_n$ and $\mathcal{H}_m$, and one of its bases consists of

$$\{\alpha_i \otimes \beta_j\}_{i,j=1}^{n,m},$$

all tensor products of vectors of the bases of Hilbert (sub)spaces $\mathcal{H}_n$ and $\mathcal{H}_m$.

Example: A quantum n-qubit register can be seen as being composed of n one-qubit systems, and as one of its bases we have all n-fold tensor products of the basis vectors/states $\{|0\rangle, |1\rangle\}$ of $\mathcal{H}_2$, that is of the vectors/states

$$|b_1\rangle \otimes |b_2\rangle \otimes \ldots \otimes |b_n\rangle$$

[2] A matrix A is called *unitary* if $A \cdot A^\dagger = A^\dagger \cdot A = I$, where $A^\dagger$ is the conjugate transpose of A.
[3] Projectors are such operators P that $P \cdot P = P$.

that are usually denoted as $|b_1b_2\dots b_n\rangle$. All such vectors form a (*computational*, or *standard*) *basis* of the Hilbert space $\mathcal{H}_{2^n}$ of n qubits.

In the classical world, each state of a composed system is composed from the states of subsystems. This is not the case in the quantum world. There are pure states of any bipartite quantum system $S_1 \otimes S_2$, represented by the tensor product of the underlying Hilbert spaces $\mathcal{H}_n$ and $\mathcal{H}_m$, that cannot be decomposed as the tensor products of the states of the underlying subsystems. Such pure states are called *entangled pure states.*

Example: The so-called EPR-state

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),$$

is an important example of an entangled state of a two-qubit register. The EPR-states is one of the four so-called *Bell states* $|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$ and $|\Psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$ that form so-called *Bell basis* in $\mathcal{H}_4$.

A measurement of entangled states may create non-local correlations and therefore entangled states used to be seen as a strange feature of quantum mechanics as the theory of the quantum world. Nowadays, entangled states are seen as an important resource of quantum information processing, what will be discussed in more details later.

Another important concept is that of a mixed state. Any probability distribution $\{(p_i, |\phi_i\rangle)\}_{i=1}^k$ on pure states is called a *mixed state.* To any such mixed state the so-called *density operator* is assigned, that is defined by

$$\rho = \sum_{i=1}^{k} p_i |\phi_i\rangle\langle\phi_i|.$$

One interpretation of a mixed state $\{(p_i, |\phi_i\rangle\}_{i=1}^k$ is that a source produces the state $|\phi_i\rangle$ with probability p_i. Any matrix representing a density operator, in a basis, is called *density matrix.* In general, a matrix ρ is a density matrix if it is Hermitian, non-negative and $Tr(\rho) = 1$.[4] Density operators are also often called *quantum states* and can be represented by points inside the Bloch sphere. A density operator ρ of a bipartite system $\mathcal{H}_A \otimes \mathcal{H}_B$ is called *entangled* if ρ cannot be written in the form $\sum_{i=1}^k p_i \rho_{A,i} \otimes \rho_{B,i}$, where $\sum_{i=1}^k p_i = 1$ and $\rho_{A,i}$ ($\rho_{B,i}$) are density operators of $\mathcal{H}_A$ ($\mathcal{H}_B$).

Density matrices are a quantum generalization of classical probability distributions.

[4]Let $\mathcal{H}$ be an n-dimensional Hilbert space and $\mathcal{B}$ be an orthogonal basis on $\mathcal{H}$. The *trace (operator)* of a linear mapping $M : \mathcal{H} \to \mathcal{H}$ is defined by $Tr(M) = \sum_{\phi\in\mathcal{B}} \langle\phi|M\phi\rangle$. In addition, if A is a matrix representation of M in a basis $\mathcal{B}$, then $Tr(M) = Tr(A) = \sum_{i=1}^n a_{ii}$, where a_{ii} is the element of the matrix A at the position (i,i). It can be shown that $Tr(M)$ does not depend on the choice of the basis.

Measurement of mixed states/density operators: If a density operator/state ρ is measured with respect to an observable A with a spectral decomposition $A = \sum_{i=1}^{k} \lambda_i P_i$, then with probability $Tr(\rho P_i)$ the classical outcome is λ_i and the state ρ collapses into the state $\frac{P_i \rho P_i}{Tr(\rho P_i)}$.

One of the profound differences between quantum and classical systems lies in the relation between systems and their subsystems. As discussed below, a state of a Hilbert space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ cannot be always decomposed into states of its subspaces $\mathcal{H}_A$ and $\mathcal{H}_B$. There is also no natural mapping from the space of linear operators on $\mathcal{H}$ into the space of linear operators on $\mathcal{H}_A$ (or $\mathcal{H}_B$).

However, density operators/states are much more robust and that is also one reason for their importance. A density operator ρ on $\mathcal{H}$ can be "projected" into $\mathcal{H}_A$ by so-called *tracing out* operation $Tr_{\mathcal{H}_B}(\cdot)$, that traces out the subsystem $\mathcal{H}_B$, to obtain the density operator (for finite dimensional Hilbert spaces):

$$\rho_{\mathcal{H}_A} = Tr_{\mathcal{H}_B}(\rho) = \sum_{|\phi\rangle, |\phi'\rangle \in \mathcal{B}_{\mathcal{H}_A}} |\phi\rangle \left(\sum_{|\psi\rangle \in \mathcal{B}_{\mathcal{H}_B}} \langle \phi, \psi | \rho | \phi', \psi \rangle \right) \langle \phi' |,$$

where $\mathcal{B}_{\mathcal{H}_A}$ ($\mathcal{B}_{\mathcal{H}_B}$) is an orthonormal basis of the Hilbert space $\mathcal{H}_A$ ($\mathcal{H}_B$).

For practical computation, it is mostly sufficient to see the tracing out operation as a linear operation such that for any bipartite system $A \otimes B$ and their states $|\phi_1\rangle$ and $|\phi_2\rangle$ of A and any states $|\psi_1\rangle$ and $|\psi_2\rangle$ of B

$$Tr_B(|\phi_1\rangle\langle\phi_2| \otimes |\psi_1\rangle\langle\psi_2|) = \langle\psi_2|\psi_1\rangle |\phi_1\rangle\langle\phi_2|.$$

Non-locality: The existence of entangled states has very important and counter-intuitive implications. Indeed, if two particles, no matter how much space-separated they are, are in the entangled EPR-state

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),$$

then a measurement of any one of them, in the standard basis, makes the EPR-state to collapse, with the same probability, to one of the states

$$|00\rangle \quad \text{or} \quad |11\rangle,$$

that is to a mixed state, and therefore the measurement (even instantaneous) of the other particle produces the same classical outcome.

Measurements of entangled states therefore produce non-local correlations. However, the non-local correlations the entangled states exhibit do not allow superluminal transmission of information and therefore do not contradict the relativity theory.

There are many ways how to create entangled states. For example, if the CNOT operator, to be introduced bellow, is applied to two separate states $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|0\rangle$, then (maximally entangled) the EPR-state is produced. This is why it is so difficult to implement such an apparently simple operation as the CNOT is. Any operation/gate that has similar property as the CNOT gate - namely that it can transform a product state into an entangled state is called an *entangling operation/gate*.

It used to be believed that two particles have first to interact in order to be in an entangled state.So-called *entanglement swapping* protocol, experimentally verified, shows that this is not so. Indeed, in case particles P_1 and P_2, and also particles P_3 and P_4, are in the EPR state, then Bell state measurement of particles P_2 and P_3 makes particles P_1 and P_4, that never interacted, to get into an entangled state, no matter how much space separated they are.

Quantum entanglement is an observable phenomenon (and can also be seen [3]). It has been observed between various quantum objects (photons, atom and photon, ...) and for the distance more than 10 km. Quantum entanglement used to be seen, till 1991, as a theoretical curiosity of no significant practical importance. Nowadays, quantum entanglement is considered as very important computation and communication resource, that it is even seen, by some, as a gold mine of current science.

As a resource entanglement allows: (a) To perform processes that are classically impossible (i.e. teleportation); (b) To speed-up (quantum) algorithms; (c) To make some communications more efficient; (d) To generate classical shared cryptographic keys in an absolutely secure way; (e) To make transmission of quantum informatio in an absolutely secure way; (f) To enlarge capacities of quantum channels; (g) To act as catalyst in some cases.

For example, if two parties share the EPR state, then one party can send to the other one, using so-called *superdense coding protocol*, safely two classical bits in one qubit - what is without shared entanglement not possible, due to the Holevo theorem.

In case of computation with pure states, use of entangled states is crucial for having polynomial time quantum algorithms that cannot be simulated efficiently on classical computers. It is not yet clear whether the same holds in case of computation with mixed states.

1.2 Superoperators

The main question we deal now with is the following very fundamental one. *What are all physically realizable operations one can perform* (at least theoretically) *on (mixed) states (to get again (mixed) states)?*

In closed quantum systems, unitary operations are the only available quantum operations. Measurements are actually outside of the closed system framework, an interface from the quantum to the classical world, but surely they are operations we consider as physically realizable. Of the main importance are quantum operations in open quantum systems. Actually, all actions that are performed in open quantum systems are quantum operations: unitary operations, measurements, channel transmissions, flow of time, noise impacts, ...

There are basically three main approaches to define what "physically realizable quantum operations" (superoperators) $\mathcal{E}$ are.

A physically motivated *axiomatic approach* says that for a Hilbert space $\mathcal{H}$ we should consider as physically realizable operations/maps on *bounded operators*, which include density operators, $\mathcal{B}(\mathcal{H}) \rightarrow \mathcal{B}(\mathcal{H})$, which are *consistent with the (statistical) interpretation of the quantum theory.* That is maps that are *linear* (to preserve superpositions), *positive* and *trace preserving* (to map density operators to density operators) and actually *completely positive* (to be sure that if a superoperator is applied to a subsystem, then the whole system is again in a quantum state).

A pragmatic approach says that superoperators are those operations that can be combined from unitary operations, adding ancillas (auxiliary quantum systems), performing (non-selective) projective measurement and discarding subsystems (ancillas) - by performing a tracing out operations.

A *mathematical approach* says that quantum operations are exactly those that have so-called *Kraus operator-sum representation*

$$\rho \rightarrow \sum_{i=1}^{k} E_i \rho E_i^{\dagger},$$

where so-called *Kraus operators* $E_i : \mathcal{H} \rightarrow \mathcal{H}$ are not necessarily Hermitian operators, but they should be positive and should form a *decomposition of the identity operator*, that is, $\sum_{i=1}^{k} E_i^{\dagger} E_i = I_{\mathcal{H}}$ – the so-called **completeness condition**.

1.3 Special quantum limitations

Major limitations on information processing, the laws of quantum world induce, are the following ones:

- *Heisenberg uncertainty principle*: There are measurements that cannot be performed simultaneously with arbitrary precision: For example, one cannot measure polarization of a photon in the vertical-horizontal basis and simultaneously in the diagonal basis

- *No-cloning and no-deletion theorems [4]* : unknown quantum states cannot be copied perfectly. For example, there is no unitary operation U in $\mathcal{H}_4$ such that $U(|\phi\rangle \otimes |0\rangle) = |\phi\rangle \otimes |\phi\rangle$ for any qubit $|\phi\rangle$ and no unitary U such that $U(|\phi\rangle|\phi\rangle) = |\phi\rangle|0\rangle$. (No-cloning is a consequence of linearity of the evolution of quantum states. Possibility of cloning (deletion) would imply superluminal communication.)

- Measurements, in general, destroy states being measured.

- There is no way to distinguish perfectly non-orthogonal states, given one copy of each.

- There is no way to distinguish perfectly mixed states with the same density matrix.

2 Quantum computation

There are two basic universal models of quantum computation: quantum Turing machines and quantum circuits. The second model is more convenient to use for the design of quantum algorithms and therefore we deal with it at first.

A quantum computation gate is specified by a unitary operation and, due to its reversibility, it has to have the same number of inputs and outputs. A quantum circuit is defined as the classical one, only all gates have to be quantum unitary operations (or measurement gates).

The following elementary unitary operators/gates play especially important role in quantum information processing:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, K = \sigma_z^{\frac{1}{2}}, T = \sigma_z^{\frac{1}{4}},$$

where σ_x, σ_y and σ_z are Pauli operators;

$$CNOT = \Lambda_1(\sigma_x),\ \text{TOFFOLI} = \text{TOF} = \Lambda_2(\sigma_x),$$

where for any one-qubit unitary U,

$$\Lambda_1(U) = \begin{pmatrix} \mathbf{I}_2 & \mathbf{0}_2 \\ \mathbf{0}_2 & U \end{pmatrix},\quad \Lambda_2(U) = \begin{pmatrix} \mathbf{I}_4 & \mathbf{0}_4 \\ \mathbf{0}_4 & \Lambda_1(U) \end{pmatrix}$$

are conditional operators in $\mathcal{H}_4$ and $\mathcal{H}_8$

$$\text{HADAMARD} = H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},\ \text{SWAP}\ \text{ and } \sqrt{\text{SWAP}},$$

where the two-qubit unitary SWAP just exchanges inputs.

A set $\mathcal{U}$ of quantum gates is called *universal* if for every unitary operation U and any $\varepsilon > 0$ there exists a quantum circuit $C_{U,\varepsilon}$ with gates from the set $\mathcal{U}$ only, that approximates U with precision ε. The concept of approximation is defined as follows: An operator

$$U : \mathcal{H}_{2^r} \rightarrow \mathcal{H}_{2^r}$$

is ε-approximated, for an $\varepsilon > 0$, by an operator

$$\bar{U} : \mathcal{H}_{2^n} \rightarrow \mathcal{H}_{2^n},$$

where $n \geq r$, using an ancilla state $|\alpha\rangle \in \mathcal{H}_{2^{n-r}}$, if for any state $|\phi\rangle \in \mathcal{H}_{2^r}$,

$$||\bar{U}(|\phi\rangle \otimes |\alpha\rangle) - U(|\phi\rangle) \otimes |\alpha\rangle|| \leq \varepsilon.$$

One of the fundamental results of quantum computation is that CNOT and all one-qubit unitary gates form a universal set of gates. Another important examples of universal sets of unitary gates are: (a) $\{\mathrm{TOF}, H, \sigma_z^{\frac{1}{2}}\}$ [5]; (b) $\{\Lambda_1(\sigma_z^{\frac{1}{2}}), H\}$ [6]. Another major result, [7] says that unitary matrices with real coefficients can be arbitrarily well approximated by circuits consisting of Toffoli and Hadamard gates only. For more about quantum computation primitives see [8]

Example: A quantum circuit on n qubits, with n parallel Hadamard operations, one for each qubit, and with the input states $|0\rangle$ on each qubit, realizes the mapping $\bigotimes_{i=1}^{n} H(|0^{(n)}\rangle)) = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle$ and therefore such a circuit creates, in one (parallel) step, an exponentially large superposition of all basis states with identical probability amplitudes.

A very important line of research is search for rich classes of quantum circuits that can be efficiently simulated on classical computers. For example, it was first shown that this holds for *Clifford circuits* that use only computational gates $CNOT, H$ and $K = \sigma_z^{\frac{1}{2}}\}$ as well as standard measurement gates [9]. This result has been recently generalised [10] and similar results have been shown for other broad classes of circuits, see [11] (using the notion of tree-width of graphs as well as formalism of contracting tensor networks) and [12] (using representation of matrix product states and formalism of one-way quantum computers) as well as their generalisation [13].

Quantum circuits with unitary gates represent "a standard view" of quantum computation - as of a process consisting of three stages: preparation of the initial state $\rightarrow$ computation using a quantum circuit $\rightarrow$ quantum measurement.

Surprisingly, any quantum computation can be performed, up to a Pauli operator, by measurements only process, at which both the creation of the initial state and computation processes can be represented by a circuit with measurement gates only.

There are two basic approaches to *measurement based* computation. In the approach based on quantum circuits with measurement-gates only, each unitary operation can be approximated, up to a Pauli operator, by a circuit with measurement gates from a universal set of measurement gates. One such set consists of measurement gates represented by the following Hermitian matrices, [14]: σ_z, $\frac{1}{\sqrt{2}}(\sigma_x - \sigma_y)$ and $\sigma_z \otimes \sigma_x$ - plus a single one-qubit ancilla.

At another measurement based approach, at so-called *one-way computing*, [15,16], the starting point is a given fixed entangled state, the so-called *cluster state*, and computation is performed by a sequence of carefully chosen one-qubit measurements, and each of them may depend on earlier measurement outcomes. The final result of the computation is determined from classical outcomes of all measurements..

2.0.1 Quantum parallelism and quantum teleportation

Two key simple discoveries are behind many surprising results in quantum computation and communication.

Quantum parallelism: If we have a mapping $f : \{0, 1, \ldots, 2^n - 1\} \Longrightarrow \{0, 1, \ldots, 2^n - 1\}$, then the mapping $f' : (x, b) \Longrightarrow (x, b \oplus f(x))$, where $x, b \in \{0, 1, \ldots, 2^n - 1\}$, is one-to-one and therefore there is a unitary transformation U_f such that $U_f(|x\rangle|0\rangle) = |x\rangle|f(x)\rangle$, for any $x \in \{0, 1, \ldots, 2^n - 1$.

Let us now consider the state $|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle|0\rangle$ that can be created in one step using a linear amount of physical resources (n Hadamard operators), as discussed above. With a **single application** of the mapping U_f we get

$$U_f|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} U_f(|i\rangle|0\rangle) = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle|f(i)\rangle.$$

Therefore, in a single step, 2^n values of f are computed and incorporated into a single state - this represents a really massive parallelism. (The catch is that not all $f(i)$ can be obtained from $U_f|\psi\rangle$.

Quantum teleportation. By teleportation, it is usually understood a process at which an object is disassembled into information that is instantaneously transmitted to a distance place and there the object is instantaneously created from the transmitted information. It is well known that in the classical world teleportation is not possible. In the quantum world, it is, in a reasonable sense.

Let us assume that two parties, say Alice and Bob, share an EPR state, by their particles P_A and P_B, and let Alice get a particle P_u in an unknown qubit state $|\phi\rangle$. It can be easily shown that if Alice measures her particles P_u and P_A in the Bell basis, then Bob's particle gets, with the same probability, into one of the states $|\phi\rangle$, $\sigma_z|\phi\rangle$, $\sigma_x|\phi\rangle$ and $\sigma_z\sigma_x|\phi\rangle$, and if Alice gets, as the result of such a measurement, information, through two bits, which of these four cases has taken place. Therefore, if Alice sends these two bits to Bob, through a classical public channel, Bob can get his particle, by multiplying its state with one or two Pauli matrices (because $\sigma_x \times \sigma_x = I, \sigma_z \times \sigma_z = I$), into the state $|\phi\rangle$. As a consequence, the unknown state $|\phi\rangle$ is "teleported" from the particle P_u to the particle P_B. This way, Alice can teleport a state she does not know to the Bob's particle the location of which she does not know either. (It is not easy to imagine how the state $|\phi\rangle$ gets from P_u to P_B. One explanation, a bit weird, due to Ch. Bennett, is that $|phi\rangle$ first propagates backwards in time from P_u to the source of the shared EPR state and from there, forwards in time, to P_B.) Teleportation protocol also demonstrates that entanglement can be viewed as providing a channel for the transmission of quantum information.)

3 Quantum algorithms

Discovery of two quantum algorithms contributed very much to a big rise of interest in QIPC - Shor's factorization algorithm from 1994 and Grover's search algorithm from 1996.

Shor's factorization algorithm from 1994 and Grover's search algorithm from 1996.

Shor's factorization algorithm makes use of the well-known fact that the factorization problem for an integer n can be reduced to the problem of finding periods of functions $a^x \bmod n$, with a as a parameter. Shor discovered that finding such periods can be done efficiently using so-called *quantum Fourier transform* that can be efficiently implemented in important cases. Quantum Fourier transform QFT_{2^n} maps basis states $|x\rangle$ of H_{2^n} into the superposition

$$\mathrm{QFT}_{2^n} : |x\rangle \rightarrow \frac{1}{\sqrt{q}} \sum_{y=0}^{2^n-1} e^{2\pi ixy/n} |y\rangle. \tag{1}$$

To factorize an integer n, Shor's algorithm goes as follows:

1. For given $n, a, q = 2^d, n^2 \leq q \leq 2n^2$ create states, using the Hadamard operations/transform and quantum parallelism,

$$\frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |n, a, q, x, \mathbf{0}\rangle \text{ and } \frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |n, a, q, x, a^x \bmod n\rangle.$$

2. By measuring the last register the last state collapses into the state

$$\frac{1}{\sqrt{A+1}} \sum_{j=0}^{A} |n, a, q, jr+l, y\rangle, \text{ or, shortly, } \frac{1}{\sqrt{A+1}} \sum_{j=0}^{A} |jr+l\rangle,$$

   where A is the largest integer such that $l + Ar \leq q$, r is the period of $a^x \bmod n$ and l is its offset.

3. In case $A = \frac{q}{r} - 1$, the resulting state has the form. $\sqrt{\frac{r}{q}} \sum_{j=0}^{\frac{q}{r}-1} |jr+l\rangle$.

4. By applying the quantum Fourier transformation we get the state

$$\frac{1}{\sqrt{r}} \sum_{j=0}^{r-1} e^{2\pi ilj/r} |j\frac{q}{r}\rangle.$$

5. By measuring the resulting state we get, for a random j, $c = \frac{jq}{r}$ and if $gcd(j, r) = 1$, what happens with sufficient large probability, then from c and q we can determine the period r.

In case $A \neq \frac{q}{r} - 1$, a more complicated classical method has to be used to find the period.

Simulation, optimisation and implementation of Shor's factorization algorithm. Three problems much bothered QIPC community. To distill crucial elements of Shor's algorithm which allow speed-up it exhibits as well to optimise and realise its implementation. It can be easily seen that Shor's algorithm has two main components: Quantum Fourier transform and modular exponentiation. Surprisingly, see [17, 18] approximate QFT (sufficient for Shor's algorithm) can be efficiently classically simulated. The key problem therefore seems modular exponentiation. Indeed, it has been shown [19] that "any classical algorithm that can efficiently simulate the circuit implementing modular exponentiation for general product input states and product state measurements on the output, allows for an efficient simulation of a whole Shor's algorithm on classical computers. Concerning optimisation, the best current outcome is that it is sufficient to use $1.5n$ qubits to factor n bit integers. Various implementation demonstrated Shor's algorithm to factor 15.

Grover's search algorithm deals with the following problem: Given is, as a black box, a function $f : \{0, 1, \ldots, 2^n - 1\} \rightarrow \{0, 1\}$ such that for exactly t inputs f has value 1. Find one of such inputs.

Classically, one needs, in the worst case, $\mathcal{O}(2^n - t)$ searches. Grover's algorithm is very simple and needs only $\mathcal{O}(\sqrt{\frac{2^n}{t}})$ searches. The algorithm starts with an equally weighted superposition $|\phi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle$ and applies on it, iteratively, $\frac{\pi}{4}\sqrt{\frac{2^n}{t}}$ times the following operation: $-H_n V_0^n H_n V_f^n$ and then performs a measurement (where V_0 is a $2^n \times 2^n$ unitary matrix that has non-zero elements only in the main diagonal and all its elements in the main diagonal are 1, except the top one that is -1; V_f is the diagonal matrix that has in the i-th raw $(-1)^{f(i)}$ and H_n is Hadamard transform in $\mathcal{H}_{2^n}$).

Efficient quantum algorithms, based on a similar idea as Shor's factorization algorithm discussed above, exist for all algorithmic problems that can be recast as so-called *Hidden subgroup problems* (HSP) for Abelian groups [20].

Given an Abelian group G and a function f that is identical on left cosets of G with respect to a subgroup G_0 and distinct on different cosets, find G_0 - its set of generators. The most important open problem in the area of quantum algorithms is to decide whether one can solve efficiently the Hidden subgroup problems also for all non-Abelian groups. Indeed, would this be the case, we would have also an efficient quantum algorithm for the very important *Graph isomorphism problem.* The existence of efficient algorithms for HSP has already been shown for a variety of non-Abelian groups. However, there are also technical results indicating that it is unlikely that HSP can be solved for all non-Abelian groups and that it is unlikely that there exists efficient algorithm for Graph isomorphism problem [21].

There is also a variety of applications of Grover's search techniques. An important generalisation of his method is known as *amplitude amplification method.*

Another powerful methods to design efficient quantum algorithms are *quantum* *random walks*, [22], and methods of adiabatic computation [23].

There is a variety of other important/interesting quantum algorithms. Of special interest are algorithms to simulate many-body quantum systems having a local Hamiltonian [24], to solve Pell equation $x^2 - dy^2 = 1$, where d is a non-square integer [25], and to solve lattice problems [26];

3.1 Quantum automata

For most of the main models of classical automata several quantum versions have been investigated. Of the main importance are various versions of quantum Turing machines, of quantum finite automata and of quantum cellular automata.

The main basic idea behind designs of quantum versions of classical automata is to consider, as the underlying Hilbert spaces, the space where configurations of the corresponding classical automata represent an orthonormal basis. An evolution step is then to transfer, in a unitary way, a basis state (a classical configuration) to a superposition of basis states representing possible next classical configurations. For a (standard) projective measurement, the underlying Hilbert space is decomposed to three subspaces: the one generated by basis states with accepting classical states, with rejecting classical states and with non-terminating classical states. A measurement is then a projection to one of these subspaces.

In case a measurement is performed after each computation step, we speak about a *many measurements mode of computation - MM*; in case a measurement is performed only at the end of computation, we speak about a *measurement once* mode of computation - MO. One-way quantum finite automata with any of these two modes of computation can accept only regular languages, but not all of them. Two-way quantum finite automata, in case of the many measurements mode of computation, can accept all regular languages and also some non-context free languages. Of a special interest are so called classical-quantum two-way finite automata that work as the classical two-way finite ones, but have also a quantum memory on states of which unitary operations and measurements can be performed. Randomized outcomes measurements bring then make from the deterministic automata the randomized ones. It is interesting that for such a model it can be proven that just one-qubit memory can significantly increase the power of automata [27]. A variety of succinctness results have also been shown, demonstrating that quantum finite automata can be exponentially more succinct than the deterministic ones [28].

Quantum multitape Turing machines, defined using the scheme described above, are the basic computational model to introduce various quantum computational complexity classes.

3.2 Quantum computation complexity

Complexity theory is a specific, powerful, informatics based and technology/physics independent, way of discovering the laws and limitations of information processing and also of the (quantum) physical world. One of its main task is to study various complexity classes. There is a variety of quantum computational complexity classes. The four main ones are:

1. Class **QP** of decision problems that can be solved in quantum polynomial time - a quantum version of the classical complexity class **P**.
2. Class **BQP** of decision problems that can be solved in quantum polynomial time with bounded error - a quantum version of the classical complexity class **BPP**.
3. **QNP** - a quantum version of the class **NP** - defined through the acceptance with positive probability.
4. **QMA** - another quantum version of the class **NP** - defined through testing using a witness.

The class **BQP** is considered now as the main class of decision problems for which feasible solutions exist.

The main relations between classical and quantum complexity classes are:

$$\mathbf{P} \subseteq \mathbf{QP} \subseteq \mathbf{BPP} \subseteq \mathbf{QBP} \subseteq \mathbf{SPACE}.$$

For related classical complexity classes and for the whole "ZOO" of complexity classes see [29].

One of the goals of quantum complexity theory is to challenge our basic intuition how physical world behaves and to understand two of the great mysteries of 20th century: what is the nature of quantum mechanics and what are the limits of computation. It would be astonishing if this would not shed light on both of them and would not bring new discoveries. The complexity theory perspective can also lead us to ask better questions about the quantum nature – nontrivial, but answerable questions, which put old quantum mysteries in a new light. Quantum computational complexity also allows to demonstrate that some physical phenomena are not possible - by showing that such phenomena would allow to solve efficiently complete problems for some computational complexity classes that are believed to be larger than the class **P**.

It is also of importance to realise that the key steps in the development of QIPC were the separations of four problems:

P1 Can we build powerful quantum computers?

P2 What could be achieved with powerful quantum computers?

P3 What are the laws and limitations of quantum information processing and communication?

P4 Can we develop a better understanding of the quantum world on the basis of the laws and limitations of QIPC?

This separation allowed the complexity theory to make substantial contributions to the attempts to solve the problems P2 and P3, especially P2, and to set as its new goal a contribution to the solution of the problem P4 (and P1).

3.3 Decoherence and quantum error correcting codes

The view of quantum computation as of a process of manipulation of pure quantum states by unitary operators is an idealistic one and valid only for the so-called *closed quantum systems* - systems having no interaction with their environment. In practical quantum computations, such systems do not really exist. What we have are *open quantum systems*, where one has to count with the destructive impact of environment called usually *decoherence*. This impact is for all known technologies so strong, and growing exponentially with time, that till 1995 there were very serious doubts whether we can really have powerful QIPC. This pessimism was, moreover, supported by a belief that, for serious physical reasons, we cannot have a quantum analogue of classical error correcting codes - so useful tool to fight with noise and errors during classical information transmission and processing.

However, it has been shown in 1995, by P. W. Shor and A. M. Steane, that, under very simple and reasonable assumptions about error models, we can have sufficiently powerful quantum error correcting codes. Namely, it has been shown that in case we can assume that errors are locally and sequentially independent, the problem of error correction can be reduced to correction of the so-called *bit errors*, represented by the Pauli operator σ_x, and *sign or phase errors*, represented by the Pauli operator σ_z.

The basic idea of quantum error correcting codes is taken from classical linear codes. Each quantum state is first encoded by replacing each basis state by an entangled superposition of a more dimensional state in such a way that if a noisy environment causes some errors, then using special auxiliary quantum systems, and a special circuit, one can detect what kind of error has happened, without destroying the erroneous state, and then correct the error(s).

An important example of an error correcting code is Shor's code with encodings

$$|0\rangle \rightarrow \frac{1}{\sqrt{8}}((|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle))$$

$$|1\rangle \rightarrow \frac{1}{\sqrt{8}}((|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle))$$

at which each qubit is replaced by a 9-qubit entangled state.

Most of important quantum error correcting codes belong to the class of *stabilizer codes*. They are defined as follows.

For a given n let $\mathcal{P}_n$ be the (Pauli) group generated by operators $\bigotimes_{i=1}^{n} P_i$, where P_i are Pauli qubit operators. This group has 4^{n+1} elements and each of its subgroups has 2^a elements for some a. To each Abelian subgroup G of the Pauli group $\mathcal{P}_n$ that does not contain the element $-I$, we can associate the subspace S_G of $\mathcal{H}_{2^n}$ of all those states in $\mathcal{H}_{2^n}$ that are common fix-points of all operators from G. Such a subspace is called a stabilizer code and all stabilizer codes are created in this way.

Fault-tolerant quantum computations. The existence of quantum error-correcting codes is not sufficient for having powerful quantum information processing. What is more needed is to have *quantum fault-tolerant computation*, at which local errors do not spread out. It was again P. Shor who showed the existence of a universal set of fault-tolerant quantum gates, for example the set of gates: $\{T, H, \sigma_z^{\frac{1}{2}}\}$ [3]. Another approach to fault-tolerant quantum computation, so-called *topological quantum computation*, derives fault-tolerance from working in the intrinsically error-protected and decoherence-free Hilbert spaces based on non-Abelian anyons [30].

Threshold theorems. The final outcome of the theory, which is behind an increasing belief that powerful quantum information processing is possible, are so called threshold theorems. They are results stating that once we are able to design very basic communication and processing elements of a certain precision, then reliable quantum information processing and communication in arbitrarily long time and distance is possible. A variety of threshold theorems, with increasingly more realistic assumptions, have been proven.

3.4 Conclusions

Quantum computation, as presented in this article, represents only a part of the important directions and outcomes in the area of QIPC. An important theoretical area is also that of quantum information theory, where the concepts of quantum entropy, various concepts of quantum information, quantum channels and their capacities play the key role. Another theoretical/experimental area of large importance is quantum cryptography, broadly understood. On the theoretical level, the key outcomes of quantum cryptography are the proofs that unconditionally secure quantum generation of shared random classical keys is possible and that no unconditional secure quantum bit commitment and oblivious transfer protocols are possible. On the experimental level, the highlight are results that more and more reliable and efficient quantum key distribution is possible for increasingly large distances that start to reach the distance of 200 km for the case fibers are used and the distance over 140 km in open air - under special circumstances. Another huge area, with a variety of results no one would believe in a couple of years ago, is experimental QIPC, especially in the area of optics, NMR, but also in solid state technologies.

3.5 BIBLIOGRAPHY

1. J. Gruska, *Quantum computing*, McGraw-Hill, 1999
2. I. I. Chuang, M. A. Nielsen, *Quantum information processing*, Cambridge university press, 2000
3. N. Brunner, C. Branciard and N. Gisin, Can one see entanglement, quant-ph/0802.0472
4. R. Jozsa, A stronger no-cloning theorem, quant-ph/0204153
5. P. W. Shor, Fault-tolerant quantum computation, *Proc. 37th Foundations of Computer Science*, 56-65, 1996
6. A. Kitaev, *Quantum computations; algorithms and error correction*, Russian mathematical Survey, 52 (6), 1191-1249, 1997
7. Y. Shi, Both Toffoli and controlled-NOT need little help to do universal computation, quant-ph/0205115, 2002
8. J. Gruska: Universal sets of quantum information processing primitives and optimal use of such primitives, *Proc. General Theory of information transfer and combinatorics*, Springer Verlag, 356-377, 2005
9. D. Gottesmann, The Heisenberg representation of quantum computers, quant-ph/9807006, 1998
10. S. Clark, R. Jozsa, and N. Linden, Generalised Clifford groups and simulation of associated quantum circuits, quant-ph/07011103
11. I. Markov, Y. Shi, Simulating quantum computation by contracting tensor networks, quant-ph/0511069
12. N. Yoran and A. J. Short, Classical simulation of limited-width cluster state quantum computation, quant-ph/0601178
13. R. Jozsa, On the simulation of quantum circuits, quant-ph/0603163
14. S. Perdrix, Towards minimal resources of measurement-based quantum computation, *New J. Physics*, 9, 200-, June 2007
15. R. Raussendorf and H. J. Briegel, A one-way quantum computer, *Phys. Rev. Lett.*, 86, 5188-5191, 2001
16. R. Jozsa, An introduction to measurement based quantum computation, quant-ph/0508124

17. D. Aharonov, Z. Landau and J. Majakovsky, The quantum FFT can be classically simulated, quant-ph/0611156

18. N. Yoran and A. J. Short, Efficient classical simulation of the approximate quantum Fourier transform, quant-ph/0611241

19. *** N. Yoran and A. J. Short, Classical simulability and the significance of modular exponentiation in Shor's algorithm, quant-ph/0706.0872

20. J. Gruska, Algebraic methods in quantum informatics, *Proc. Algebraic Informatics*, Springer, LNCS 4728, 87-111, 2007

21. S. Hallgren, C. Moore, M. Roetteler, A. Russel and P. Sen, Limitations of quantum coset states for graph isomorphism, *Proc. 38th Symposium on Theory of Computing*, 604-617, 2006

22. A. M. Childs, R. Cleve, E. Deotto, E. Farhi, S. Gutmann and D. A. Spielman, Exponential algorithmic speedup by quantum walks, quant-ph/0209131, 2002

23. W. van Dam, M. Mosca, U. Vazirani: How powerful is adiabatic quantum computation, *Proc. 42th Foundations of Computer Science*, 2001, 279-287

24. D. S. Abrams and S. Lloyd: Simulation of many-body Fermi systems on universal computers , quant-ph 9703054

25. S. Hallgren, Polynomial time quantum algorithms for Pell's equation and the principal ideal problem, *Journal of ACM*, 54 (1), 1-19, 2007

26. O. Regev, Quantum computation and lattice problem, *SIAM Journal of Computing*, 33 (3) 738-760, 2004

27. A. Ambainis and J. Watrous, Two-way finite automata with quantum and classical states, quant-ph/9911009, 1999

28. J. Gruska: Descriptional complexity issues in quantum computing, *Journal of Automata, Languages and Combinatorics*, 5 (3), 191-218, 2000

29. S. Aaronson, Complexity ZOO, 2003
http://qwiki.stanford.edu/wiki/Complexity_Zoo

30. **** A. Yu. Kitaev, Fault-tolerant quantum computation by anyons, *Ann. Phys.*, 303, 2-, 2003

3.6 READING LIST

J. Gruska, *Foundations of computing*, Thomson International Computer Press, 1997
P. Kaye, R. Laflame and M. Mosca, *An introduction to quantum computing*, Oxford University Press, 2007
A. Peres, *Quantum theory: concepts and methods*, Kluwer Academic Publisher, 1993
D. Brußand G. Leusch, *Lectures on quantum information*, Willey, 2007