Physical Limits and Information Bounds of Micro Control. Part 2: Quantum Soft Computing and Quantum Searching Algorithms.

S.V.Ulyanov
Yamaha Motor Europe N.V.
Polo Didattico di Crema, Via Bramante, 65-26013, Crema (CR) - Italy
Phone: +39-0373-898-227; Fax: +39-0373-898-227; E- mail: sergei.ulianov@st.com

G.Degli Antoni
Polo Didattico e di Ricerca di Crema
Via Bramante, 65-26013 Crema (CR) - Italy
Phone: +39-0373-898-205; Fax: +39-0373-898-253; E-mail: gda@dsi.unimi.it

K.Yamafuji
Dept. of Mechanical and Control Eng.
University of Electro-Communications
1-5-1 Chofu, Chofugaoka ,182 Tokyo, Japan
Phone: +81-424- 83-2161; Fax: +81-424-84-3327; E-mail: yamafuji@yama.mce.uec.ac.jp

T.Fukuda
Dept. of Micro System, Dept. of Mechanics- Informatics, Nagoya University
Furo-cho, Chikusa-ku, Nagoya
Phone:+81-52-789-3116; Fax: +81-52-789-3409; E- mail: fukuda@mein.nagoya_u.ac.jp

G.G.Rizzotto
STMicroelectronics
20041 Agrate Brianza-Italy, Via C. Olivetti, 2
Phone:+39-39-603- 5918; Fax: +39-39-603-6129; E-mail: gianguido.rizzotto@st.com

I.Kurawaki
Yamaha Motor Europe N.V.
Polo Didattico di Crema, Via Bramante, 65-26013, Crema (CR) - Italy
Phone: +39-0373-898-227; Fax: +39-0373-898-227

Japan, Nagoya, November 25-28, 1998

Abstract

Principles of quantum soft computing, models of fast quantum searching algorithms and the possibility of its applications for intelligent control of micro–systems are introduced. The description problem of *searching* and *decision–making support processes* from more fundamental mutual positions of the new informational technologies and a modern physics, *information physics*, are discussed:

1. in the quantum information theory–the *information complexity* theory of *random symbolic sequences, computation complexity, quantum searching algorithms*;

2. in the modern physics–*non–equilibrium thermodynamics* and *quantum mechanics*.

1 Introduction

The quantum search algorithms for the support of decision–making process in micro control systems require the fast computers and algorithms with parallel data processing. From a computational point of view all modern computers look alike: A fundamental thesis of computer sciences (the modern form of the Church- Turing machine) asserts that this is inevitable in a deep sense. Any computer can be simulated with a most polynomial factor slowdown by a probabilistic Turing machine (PTM). The first credible challenge to this thesis was posed by *quantum computation*: Feynman [1, 2] pointed out that for simulating efficently a quantum mechanical system on a computer, we need (perhaps) a computer based on quantum physical laws and principles. Deutsch defined two formal models for quantum computers: 1) the quantum Turing machine (QTM); and 2) the quantum computational networks. At this stage it will be necessary to include in the description of computers quantum phenomena, such as *quantum superposition, quantum interference and quantum entanglement* [1, 2]. The background of quantum computation are the physical laws of quantum information theory [1]. The physics of information and computation has been a recognized discipline for several last decades. Information is something that is encoded in the state of a physical system; a computation is something that can be carried out on an actual physical realizable device. Rolf Landauer [18, 19] pointed out that "information is physical" and the erasure of information is necessarily a dissipation process (erasure always involves the compression of phase space, so it is irreversible). The logical gates used to perform computation are typically irreversible. As example, the $NAND$ gate $(a, b) \rightarrow \neg(a \wedge b)$ has two input bits and one output bit and it can not recover an unique input from the output. At least a work $W = kT \ln 2$ is needed to operate the gate. It is possible to construct a reversible version of the $NAND$ gate that preserves all the information about the input. For example, the Toffoli gate $(a, b) \rightarrow (a, b, c \oplus a \wedge b)$ is a reversible 3–bit gate that flips the third if the first two both take the value 1 and does nothing otherwise. The third bit becomes the $NAND$ of a and b if c =1. It is possible to transform an irreversibble computation into a reversible one by replacing the $NAND$ gates by Toffoli Gates. This computation could be done (in principle) with negligible dissipation. In quantum mechanics information source are described by truly random process, in contrast, there is no place for true randomness in deterministic classical dynamic. Furthermore, in quantum mechanics, noncommuting observables can not simultaneously have precisely defined values (the Heisenberg's uncertainty principle): a measurement of one observable O_1 will necessarily influence the outcome of a subsequent measurement of an observable O_2, if O_1 and O_2 do not commute. The act of acquiring information about physical system alters inevitably the state of system. There is no counterpart of this limitation in classical physics. Moreover, if we could make a perfect copy of a quantum state, we could measure an observable of the copy without disturbing the original and we could defeat the principle of disturbance. But the acquiring of information without causing a disturbance is connected with another essential distinction between classical and quantum information : " quantum information cannot be copied with perfect fidelity" (the no-cloning theorem). John Bell (1964) introduced in a more deep way in what quantum information differs from classical information. Bell showed that the predictions of quantum mechanics cannot be reproduced by any local hidden variable theory. In this case quantum information can be encoded in local correlations between the different parts

of a physical system (correlation with no classical counterpart). Entanglement state is an example of this phenomenon. The discrete character of quantum-mechanical systems such as photons, atoms, and spins allows them to register ordinary digital information. A left-circularly polarized photon can encode a 0, for example, while a right- circularly polarized photon can encode a 1. Quantum systems can also register information in ways that classical digital system cannot: a transversely polarized photon is in a quantum superposition of left and right polarization and in some sense encodes both 0 and 1 at the same time. Even more surprising from the classical perspective are so-called entangled states, in which two or more quantum system are in superposition of correlated states, so that two photons can encode, for example, 00 and 11 at once. Such entangled states behave in ways that apparently violate classical presentations about locality and causality (without actually violating physical law). Information stored on quantum systems that can exist in superposition and entangled states is called quantum information. The unit of quantum information is the quantum bit (or qubit), the amount of quantum information that can be registered on a single two-state variable such as a photon's polarization or a neuron's spin. A quantum computer is a new type of computer which can solve very efficiently problems such as factoring and database searching. Such *quantum computers with quantum search algorithms could solve problems that are not resolvable on classical computers.* It might be possible to combine quantum mechanical algorithms with efficient database algorithms that make use of specific properties of the database. There exist fast quantum mechanical searching algorithms [22] that does not use any knowledge about the problem . The *Shor's* algorithm [26] is the fast quantum mechanical algorithm that make use the known structure of the problem at hand. It might be also possible to combine the searching algorithms [22] with other quantum mechanical algorithms [5, 6, 25] to design even faster algorithm [26]. Quantum mechanical algorithms can speed up a range of search applications over unsorted data. Quantum mechanical systems can be in superposition of states and simultaneously examine multiple objects. By properly adjusting the phase of various operations, successful computations reinforce each other while others interfere randomly. As result, the desired search object can be obtained between N objects in only $O(\sqrt{N})$ accesses to the database. Any classical algorithm (deterministic or probabilistic) will clearly take $O(\sqrt{N})$ steps since on the average it will have to examine a large fraction of the N records [23, 24, 25]. A good prototype of quantum mechanical algorithms are probabilistic (simulated annealing) algorithms. In these algorithms, instead of having the system in a specific state, we have it in a distribution over various states with a certain probability of being in each state. At each step, there is a certain probability of making a transition from one state to another. The probability vector describe the distribution of probabilities over various states and the evolution of the system is obtained by pre- multiplying this probability vector by a state transition matrix. Knowing the initial distribution and the state transition matrix, it is possible in principle to calculate the distribution at any instant in time. A quantum computer consists of atomic particles which obey the laws of quantum mechanics. The complexity of a quantum system is exponential with respect to the number of particles. Performing computation using these quantum particles in an exponential amount of calculation in a polynomial amount of space and time [1, 4, 5]. This quantum parallelism is only applicable in a limited domain: errors limit the effectiveness of any physical realization of a quantum computer. A quantum computer is subject of two different types of errors: inaccuracies and decoherence. Decoherence occurs when a

quantum computer interacts with the environment. This interaction destroys the quantum parallelism by turning a quantum calculation into a classical one. The inaccuracies, as the other type of error, accumulates over time and destroys the results of the calculation. Very recent results of *P.W. Shor* [1, 2] have shown the existence of quantum mechanical error correcting codes which enable transmission of data even in the presence of noise. The design of error free quantum gates still remains an unsolved problem [29]. The simulation results show that the error rate per gate is on the order of 10^{-6} for a trapped ion quantum computer whose noise is kept below $\pi/4096$ per gate and with a decoherence rate of 10^{-6}. Previous studies have shown that a quantum computer can factor more efficiently than a classical computer if the error rate is of order 10^{-6}. In this report we discuss the principles of quantum soft computing based on Genetic Algorithms (GA) and quantum searching algorithms for micro– nano–robotics.

2 Quantum Computing

2.1 Principles of Quantum Mechanics for Quantum Computation

Quantum dualism: Unhindered quantum system acts like a wave; upon interaction with the environment, it acts like a particle. A quantum system exhibits a Janus–like dualism as it evolves. Classically continuous variables such as energy, angular momentum and charge come in discrete unit called quanta. Wave-like character of quantum system is used for the time evolution description of fairly large systems with no "measurement" (or, to be more precise, no decoherence or interaction with the environment). The discrete character of quantum systems such as photons, atoms, and spins allows them to register ordinary digital information.
Quantum Superposition, Entangelment and Interference: The quantum state at all times has components corresponding to some or all of the possible classical states. This quantum effect is known as a *superposition state*. A computer built upon quantum rules could process different inputs in *parallel massive* and produce a superposition of outputs. In this case a quantum computer is a *physical machine* that can accept input states which represent a coherent superposition of many different possible inputs and subsequently evolve them into a corresponding superposition of outputs. *Quantum entanglement* allows one to encode data into non-trivial multiparticle superpositions of some pre-selected basis states, and *quantum interference* (which is a dynamic process) allows one to evolve initial quantum states (as inputs) into final states (as outputs) modifying intermediate multiparticle superpositions in some prescribed way. Quantum computer use the quantum interference of different computational paths to enhance correct outcomes and suppress erroneous outcomes of computations. A common pattern underpinning quantum algorithms can be identified when quantum computation is viewed as multiparticle interference. Multiparticle interference (unlike single-particle interference) does not any classical analogue and can be viewed as inherently quantum process.
Quantum Computation and Physics : The development a quantum information processor it would needed first of all discrete, robust quantum states. Five candidates are considered: photons, atoms or ions, quantum dots, magnetic moments or spins, and super-conducting rings. At all times, the quantum state has components corresponding to some or all of the possible classical states. This aspect is known as a superposition state. Phenomena

such as quantum interference and quantum entanglement can be exploited for computation. Quantum computers can accept input states that represent a coherent superposition of many different possible inputs and subsequently evolve them into a corresponding superposition of outputs. Computation (i.e., a sequence of unitary transformations) simultaneously affects each element of the superposition, generating a massive parallel data processing, albeit within one piece of quantum hardware. Proposed experimental realizations of quantum logic gates, including cavity quantum electrodynamics, quantum dot arrays, and the selective excitations of trapped ions [1, 2]. So, a computer built upon quantum rules could process different inputs in parallel and produce a superposition of outputs. The expectation is that such a computer could solve problems that are not resolvable on classical computers. A quantum computer in theory could be constructed from elementary reversible logic gates, which would be the quantum version of reversible classical gates. For building physically a quantum processing system are present two main obstacles: incorrect reversible evolution and decoherence. The idea of error correction is suggested as a way to get around these obstacles.

Physics of Quantum Mechanical Algorithms: Just like classical algorithms, quantum mechanical algorithms work with a probability distribution over various states. Unlike classical systems, the probability vector does not describe the system completely. It is needed (in order to completely describe the system) the amplitude in each state, which is a complex number. In analogy with classical systems the evolution of the quantum system is obtained by pre-multiplying this *amplitude* vector (that describes the distribution of amplitudes over various states) by a transition matrix, the entries of which are complex in general [24, 25]. In order to conserve probabilities, the state transition matrix must be unitary. In quantum computer, the logic circuitry and time steps are essentially classical, only a memory bits that hooped the variables are in quantum superpositions. Quantum mechanical operations that can be carried out in a controlled way are unitary operations that act on a small number of bits in each step. The quantum search algorithm is a sequence of such unitary operations on a pure state, followed by a measurement operation.

Remark 1: Probability amplitudes are complex numbers (of modulus not greater than unity); the corresponding probability is obtained by taking a modulus squared of the probability amplitude. This way of calculating probabilities gives the quantum computation the novel non–classical feature of quantum interference. For example, let Ψ_k be arbitrary wave functions as the solution of corresponding Schrödinger equation:

$$\imath\hbar\frac{\partial|\psi_k\rangle}{\partial t} = H|\psi_k\rangle$$

then

$$|\Psi\rangle = \sum_{k=1}^{\infty}\alpha_k\psi_k$$

defines a new wave function. This is the so–called superposition principle of state Ψ_k in quantum mechanics. (It is nothing but the linearity of the space of wave functions). It is claimed in quantum mechanics that $|\Psi|^2 = \Psi\overline{\Psi}$ is a probability distribution density. Let us consider the simplest case of two wave functions $\psi_1+\psi_2$, where we neglect "normalization" for simplicity. Then

$$|\psi_1+\psi_2|^2 = |\psi_1|^2 + |\psi_2|^2 + 2Re(\psi_1\overline{\psi_2})$$

The real part $Re(\psi_1\overline{\psi_2})$ of cross term is called "interference" of the wave function ψ_1 and ψ_2. If a particular final configuration can be reached via a two different paths with amplitudes α and $(-\alpha)$, then the probability of reaching that configuration is $|\alpha - \alpha| = 0$, despite the fact that the probability for the computation to follow either of the two paths separately is $|\alpha|^2$ in both cases. Furthermore, a single quantum computer can follow many distinct computational paths in superposition and produce a final output depending on the interference of all of them. This is in contrast to a clasical probabilistic Turing machine (PTM), which follows only some single (randomly chosen) path.

2.2 Information Theory Point of View: Bits and Qubits

The fundamental unit of information in classical (Shannon) theory is the bit. All classical information can be encoded in bits and any classical computation can be reduced to fundamental operations that flip bits $(0 \rightarrow 1, 1 \rightarrow 0)$. The bit in quantum theory of information is replaced by a more general construct : the quantum bit, or qubit. The qubit is the basic unit of storage in a quantum computer. Because of the properties of quantum mechanics, the qubit differs from the classical bit. Th qubit can be found in both two states (zero and one) simultaneously–the superposition of zero and one states. The superposition state lasts until we perform an external measurement. This measurement determines without doubt the value of the qubit. The orthonormal basis states for two dimensional complex vector space are $|0\rangle$ and $|1\rangle$, and the state of a qubit (for pure quantum state) can be any normalized vector as

$$\alpha|0\rangle + \beta|1\rangle \tag{1}$$

where α and β are complex numbers and $|\alpha|^2 + |\beta|^2 = 1$. If the state of the qubit is either $\alpha = 1$ and $\beta = 0$ or $\alpha = 0$ and $\beta = 1$, then a classical bit can be viewed as the special case of the qubit. If the value of the (1) is measured, the result is 0 with probability $|\alpha|^2$ and 1 with probability $|\beta|^2$. A string of n classical bit can take any one of 2^n possible values; for n qubits, these 2^n classical strings are regarded as the bases states for a complex vector space of dimension 2^n and a pure state of n qubits is a normalized vector in this space.

2.3 Quantum Transformation and Logic Gates

A quantum computation is a sequence of transformations performed on the qubits contained in quantum registers [1, 2]. A transformation takes an input quantum state and produces a modified output quantum state. Typically transformations are defined at gate level, i.e. transformations which perform logic functions. (The simulator performs each transformation by multiplying the 2^M dimensional vector by $2^M \times 2^M$ transformation matrix). The basic gate used in quantum computation is the CONTROLLED-NOT, i.e. esclusive OR gate. The CONTROLLED-NOT gate is a two bit operation between a control bit and a resultant bit. The operation of gate leaves the control bit unchanged, but conditionally flips the resultant bit based on the value of the control bit.

2.4 Data Processing in Quantum Computing

In quantum computing n qubits are initially prepared in an algorithmic simple input state, such as $|in\rangle = |0\rangle|0\rangle \ldots |0\rangle$. Then a unitary transformation U is applied to the input state

$|in\rangle$, yielding an output state as $|out\rangle = U|in\rangle$. A set of commuting observables $O_1, O_2, \ldots$ is measured in the output state. The measured values of these observables constitute, finally the outcome of the computation. The quantum computation is not deterministic, since the output state is not necessary an eigenstate of the measured observables. The same computation, performed many times, will generate a probability distribution of possible outcomes. That is the j^{th} qubit $|\ \rangle_j$ is protected onto the computational basis $\{|0\rangle_j, |1\rangle_j\}$.

2.5 The Complexity and Universality of Quantum Computing

Rules that specify how the transformation U is constructed characterize the complexity of quantum computation. In quantum mechanics operator U is expressed as a product of elementary unitary transformation (quantum gates) that acts on a bounded number of qubits independent from n. According to results [1, 2] "almost any" *two-qubit unitary transformation, together with qubit swapping operations, is universal* for quantum computation. If given a generic 4×4 unitary matrix $\widetilde{U}$ as $\widetilde{U}^{i,j}$ acting on the i^{th} and j^{th} qubits according to:

$$\widetilde{U}^{i,j} : |\alpha_i\rangle_i |\alpha_j\rangle_j \mapsto \widetilde{U}_{\alpha_i \alpha_j \alpha'_i \alpha'_j} |\alpha'_i\rangle_i |\alpha'_j\rangle_j \tag{2}$$

Then any $2^N \times 2^N$ unitary transformation U can be approximated to arbitrary precision by a finite string of $\widetilde{U}^{i,j}$s as:

$$U \cong \widetilde{U}^{i_T,j_T} \ldots \widetilde{U}^{i_2,j_2} \widetilde{U}^{i_1,j_1} \tag{3}$$

The length T of this string (or "time") is a measure of the complexity of the quantum computation [1]. Determing the precise string $\widetilde{U}^{i,j}$s that is needed to perform a particular computation task may itself be computational demanding.

Remark 2 To have a reasonable notion of complexity, it should require that a conventional computer (as a Turing machine) generates the instructions for constructing the unitary transformation . The complexity of the computation is actually the sum of the complexity of the classical computation and the complexity of the quantum computation. In this case say [1] that a problem is tractable on a quantum computer if the computation that solves the problem can be performed in a time that is bounded from above by a polynomial in n, the number of qubits contained in the quantum register. This notion of tractability is largely independent of the details of the design of the machine and choice of the fundamental quantum gates. The quantum gates of one device can be simulated to polynomial accuracy in polynomial time by the quantum gates of another device.

Remark 3. A classical computer can simulate a quantum computer to any desired accuracy. However, the classical simulation may involve matrices of exponentially large size and so may take an exponentially long time. Quantum computers may be able to solve certain problems far more efficiently than classical computers.

2.6 Massive Quantum Parallelism

According to the Detsch result [1, 2] a quantum computer can exploit "massive quantum parallelism". As example, if we are interested in studying the properties of a function f

defined on the domain of nonnegative integers $0, 1, 2, \ldots, 2^L - 1$ then a unitary transformation U_f can be constructed that computes efficiently f as:

$$U_f : |(i_{L-1}i_{L-2}\ldots i_1 i_0)\rangle_{in}|(00\ldots 0)\rangle_{in} \mapsto |(i_{L-1}i_{L-2}\ldots i_1 i_0)\rangle_{out}|f(i_{L-1}i_{L-2}\ldots i_1 i_0)\rangle_{out} \tag{4}$$

Here $(i_{L-1}i_{L-2}\ldots i_1 i_0)$ is an integer expressed in binary notation and $|(i_{L-1}i_{L-2}\ldots i_1 i_0)\rangle$ denotes the corresponding basis state of L qubits. The operator U_f has been constructed to leave the state in the $|(\ )\rangle_{in}$ register undisturbed to ensure that is indeed a reversible operation, since the function f might not be invertible. According to the principle of superposition, operator (4) defines the action of U_f on each of 2^L basis states and on all states of a 2^L dimensional Hilbert sates. Starting with the state $|(00\ldots 0)\rangle_{in}$ and applying single–qubit unitary transformations to each of L qubits it is easy to prepare from (1) the state:

$$(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle)^L = \frac{1}{2^{L/2}}\sum_{i_{L-1}=0}^{1}\cdots\sum_{i_1=0}^{1}\sum_{i_0=0}^{1}|i_{L-1}i_{L-2}\ldots i_1 i_0\rangle_{in} \equiv \frac{1}{2^{L/2}}\sum_{x=0}^{2^L-1}|x\rangle_{in}$$

an equally weighted coherent superposition of all of the 2^L distinct basis states. With this input the action of U_f prepares the entangled quantum state

$$|\psi_f\rangle \equiv \frac{1}{\sqrt{2}}\sum_{x=0}^{2^L-1}|x\rangle_{in}|f(x)\rangle_{out} \tag{5}$$

Deutsch called the highly entangled quantum state (5) as the effect of "massive parallelism". So applying the unitary transformation we will run the computation only once, in a sense that this state encodes the value of the function f for each possible value of the input variable x . If we do a measurement on all the qubits of the input register and obtain the result $x = a$, a subsequent measurement on the output register would reveal with certainity the value $f(a)$.

Remark 4. The measurement, unfortunately, will destroy the entangled quantum state, and the procedure cannot be repeated. Deutsch emphasized, however, that certain global properties of the function f can be extracted from the state (5) by making appropriate measurements [1, 2].

3 Quantum Mechanical Operations and // Fast Quantum Searching Algorithms

Such a quantum computer, as a quantum system, possesses, during all its existence, components corresponding to different classical possibilities. So a superposition state of a quantum bit (qubit), would contain a component corresponding to the value {0} and a component corresponding to {1} at the same time: the state is neither wholly zero nor wholly one, as must apply for a classical bit. A computer built upon quantum rules could processes the different inputs in parallel to produce a superposition of outputs. It is already known that this parallelism would enable a quantum computer to attack some problems which are intractable on any classical machine. (The expectation is that such

a computer could solve problems that are not resolvable on classical computers.) The quantum algorithms of Deutsch , Simon and Shor are described in a way which highlights their dependence on the Fourier transform. The principal quantum algorithms which provide an exponential speed-up over any known classical algorithms for the corresponding problems are Deutsch's algorithm, Simon's algorithm and Shor's algorithm. The large unitary operation is the Fourier transform. The quantum searching algorithm of Grover is also based on the Fourier transform [22, 23].

3.1 Quantum Operations for Search Algorithms

Three elementary unitary operations are used in the search algorithm. The first is the creation of a configuration (superposition) in which the amplitude of the system being in any of the $N(=2^n)$ basic states of the system is equal; second is the Walsh–Hadamard (Fourier) transformation operation, and the third is the selective rotation of the phase of different states [22, 23, 24, 25].

The Creation of Superposition. A basic operation in quantum computing is that of a "fair coin flip" (the operation M) performed on a single bit by the matrix

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

A bit in the state 0 is transformed into a superposition in the two states: $(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$. Similarly a bit in the state 1 is transformed into $(\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}})$, i.e the magnitude of the amplitude in each state is $\frac{1}{\sqrt{2}}$ but the phase of the amplitude in the state 1 is inverted. The phase *does not have an analog* in classical probabilistic algorithm. It comes about in quantum mechanics since the amplitude are in general complex.

Remark 5. As mentioned previously (see *Remark 4*), the probabilities are determined by the square of the absolute value of the amplitude in each state. Hence the probabilities of the two states in both cases (i.e. when the amplitudes are $(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$ and when they are $(\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}})$) are equal. And yet the distribution have *very different* properties. For example multiplying M to the distribution $(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}})$ results in the configuration being in the state 0; applying M to the distribution $(\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}})$ results in the system being in the state 1. Two distributions that had the *same* probability distributions over all states, now have *orthogonal* distributions. This illustrates the point that, in quantum mechanics, the complete description of the system requires the amplitudes over all states, just the probabilities are not enough [22, 23, 24, 25]. In a system in which the states are described by n bits (it has $N = 2^n$ possible states), we can perform the transformation M on each bit independently, changing in this way the state of the system. The state transition matrix representing this operation will be of dimension $2^n \times 2^n$. In this case the initial configuration was the configuration with all n bits in the first state, the resultant configuration will have an identical amplitude of $2^{-n/2}$ in each of the 2^n states. This is a way to create a superposition with the same amplitude in all states 2^n.

Walsh–Hadamard (the Fourier) Transformation Operation. The starting case is another one of the 2^n states, i.e., a state described by an n bit binary string with some 0–s and some 1–s. The result of performing the transformation M on each bit will be

a superposition of states described by all possible n bit binary string with amplitude of each state having a magnitude equal to $2^{-n/2}$ and sign either $(+)$ or $(-)$. To deduce the sign, observe that from definition of the matrix M the phase of the resulting configuration changes when a bit that was previously a 1 after the transformation remains a 1 . Let be $\overline{x}$ the n–bit binary string describing the starting state and $\overline{y}$ the n–bit binary string describing the resulting string, the sign of the amplitude of $\overline{y}$ is determined by the parity of the bitwise dot product of $\overline{x}$ and $\overline{y}$, i.e., $(-1)^{\overline{x}\cdot\overline{y}}$. This transformation is refered to as the $C(w)$. This operation (or a closely related operation called the Fourier transformation) is one of the things that makes quantum mechanical algorithms more powerful than classical algorithms and forms the basis for most significant quantum mechanical algorithms.

The Selective Rotation of the Phases of States. The third transformation that we will need is the selective rotation of the phase of the amplitude in certain states, which is of the following form for a two– state system

$$\begin{pmatrix} e^{\jmath\phi_1} & 0 \\ 0 & e^{\jmath\phi_2} \end{pmatrix}$$

where $\jmath = \sqrt{-1}$ and ϕ_1, ϕ_2 are arbitrary real numbers.

Remark 6. Note that, unlike the Walsh-Hadamard transformation and other state transition matrix, the probability in each state stays the same since the square of the absolute value of the amplitude in each state stays the same.

3.2 The Black–Box Model and Tight Bounds on Quantum Search

Many quantum algorithms can be naturally expressed in the black–box model, such as the algorithm due to Grover or Simon. The black–box model of computation arises when one is given a black box containing N–tuple of boolean variables $\vec{x} = (x_0, x_1, \ldots, x_{N-1})$.The box is equipped to output x_i on input i. In this case we wish to determine some property of $\vec{x}$ accessing the x_i only through the black box. Such a black–box access is called a *query*. A property of $\vec{x}$ is any boolean function that depends on $\vec{x}$, i.e. a property is a function $f : \{0,1\}^N \mapsto \{0,1\}$ We want to compute such properties using as few queries as possible. Consider, for example, the case where the goal is to determine whether or not $\vec{x}$ contains at least one 1, so we want to compute the property $OR(\vec{x}) = x_0 \vee \ldots \vee x_{N-1}$. It is well known that the number of queries required to compute OR by any classical(deterministic or probabilistic) algorithm is $\Theta(N)$. Grover [22, 23] discovered a remarkable quantum algorithm that making queries in superposition, is able to compute OR with small error probability using only $O(\sqrt{N})$ queries. This number of queries is shown to be asymptotically optimal [1].

Simon's algorithm [1, 2], (in which one is given a function $\tilde{x} : \{0,1\}^N \mapsto \{0,1\}^N$), technically can also be viewed as a black–box $\vec{x} = (x_0, x_1, \ldots, x_{N-1})$ with $N = n2^n$. The black–box $\vec{x}$ satisfies a particular promise, and the goal is to determine whether or not $\vec{x}$ has some other property. Simon's quantum algorithm is proven to yield an exponential speed–up over classical algorithms in that it makes $(\log N)^{O(1)}$ queries, whereas every classical randomized algorithm for the same function must take $N^{\Omega(1)}$ queries. The promise means that the function $f : \{0,1\}^N \mapsto \{0,1\}$ is *partial* (it is not defined on all $\vec{x} \in \{0,1\}^N$). The function OR is *total*, however, the quantum speed–up is only quadratic.

The analysis of the black–box complexity of several functions and classes of functions in the quantum computation setting show that the kind of exponential quantum speed–up that Simon's algorithm achieved for a partial function cannot be obtained by any quantum algorithm for any total function: at most a polynomial speed–up is possible [30].

They are considered three different settings for computing f on $\{0,1\}^N$ in the black–box model: 1) the exact setting; 2) the zero– error setting and 3) the two–sided bounded–error setting. In the exact setting, an algorithm is required to return $f(\vec{x})$ with certainty for every $\vec{x}$. In the zero–error setting, for every $\vec{x}$, an algorithm may return "inconclusive" with probability at most 1/2, but if it returns an answer, this must be the correct value of $f(\vec{x})$ (algorithms in this setting are sometimes called Las Vegas algorithms). And, in the two–sided bounded–error setting, for every $\vec{x}$, an algorithm must correctly return the answer with the probability at least 2/3 (algorithms in this setting are sometimes called Monte Carlo algorithms) [30].

Consider the OR–function, which is related to database search. By Gover's search algorithm, if at least one x_i equals 1, we can find an index i such that $x_i = 1$ with high probability of success in $O(\sqrt{N})$ queries. This implies that we can also compute the OR–function with high probability of success in $O(\sqrt{N})$. If we want to get rid of the probability of error and want to compute the OR–function exactly or with zero–error using $O(\sqrt{N})$ queries then the result is negative. A quantum network for exact or zero–error search requires N queries [30].

4 Example 1

Quantum computation of period τ for the function

$$f(t) \equiv f(t+\tau), \tau \ll 2^L.$$

By exploiting quantum inerference, a quantum computer can determine the period of a function efficiently. This computation of the period for a given state (5) can be performed by manipulating (and ultimately measuring) only the state of the input register (we do not disturbe the output register). The trace over the unobserved state of the output register, obtaining the mixed density matrix as

$$\rho_{in,f} \equiv tr_{out}(|\psi_f\rangle\langle\psi_f|) = \frac{1}{\tau}\sum_{k=0}^{\tau-1} |\psi_k\rangle\langle\psi_k|$$

where

$$|\psi_k\rangle = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1} |x = k + \tau j\rangle_{in}$$

is the coherent superposition of all the input that is maped to a given output and $N-1$ is the greatest integer less than $(2^L-1)/\tau$. The unitary transformation (the Fourier transform)

$$\Phi : |x\rangle \mapsto \frac{1}{2^{L/2}}\sum_{y=0}^{2^L-1} e^{2\pi\imath xy/2^L}|y\rangle \tag{6}$$

as Shor showed [26], can be composed from a number of elementary quantum gates that is bounded from above by the polinomial in N. Apply Φ to the input register and measure its value y, the outcome of the measurement is governed by the probability distribution [1] as

$$P(y) = \frac{N}{2^L} \left| \frac{1}{N} \sum_{j=0}^{N-1} e^{2\pi \imath y \tau j / 2^L} \right|^2 \tag{7}$$

This probability distribution is strongly peaked about values of y of the form

$$\frac{y}{2^L} = \frac{(integer)}{\tau} \pm O(2^{-L}) \tag{8}$$

where the integer is a random number less than τ. The peaking of the probability distribution in (7) is quite robust. As long as the errors in the phase occurring in the sum over j are small compared to 2π, constructive interference will occur when the condition (8) is satisfied. If τ is known to be less than $2^{L/2}$ then each time we prepare the state (5), apply the Φ to the input register, and then measuring the input register, we will have a probability of order $1/\log\log\tau > 1/\log L$ (it is known that if positive integers τ and $s < \tau$ are randomly selected, then τ and s will be relative prime with a probability of order $1/\log\log\tau$) of successfully inferring from the measurement of the period τ of the function f. If we carry out this procedure a number of times that is large compared to $\log L$, we will find the period of f with probability close to one.

Remark 7. Equation (6) are not only the quantum parallelism already mentioned, but also quantum entanglement and, finally, quantum interference. Each value of $f(x)$ retains a link with the value of x which produced it, through the entanglement of the x and y registers in (6). The "magic" happens when a measurement of the y register produces the special state $|\psi\rangle$ as in (5) in the x register, and it is a quantum entanglement which permits this. The final Fourier transform can be regarded as an interference between the various superposed states in the x register (compare with the action of a different grating).

5 Quantum Soft Computing Based on GA

Genetic Algorithm (GA) include three main operations : selection, crossover and mutation. GA have been effective in approximately solving many hard problems and as quantum computing include some NP-complete problems. GA can be performed on quantum computer [31]. And GA use complete isolated space of solutions. In quantum computing it is possible to use the states of complex (different) spaces of possible solutions as superposition of entanglement states. The power of quantum soft computing is in the state optimization of dynamic micro system on all possible solution spaces. In GA a chromosome in the population is assumed to be coded with binary strings with length n. The total number of this strings is 2^n. A small number $m \ll 2^n$ are chosen to be usually in the population. For this case a chromosome in GA corresponds to a possible state in a quantum computer. A unitary transformation will emulate the crossover operator and the mutation operator can be described by changing the bit at a certain position (or positions). The selection operator is based on the fitness values of chromosomes and will be equivalent to a suitable Hamiltonian. For the solution of optimization problem are needed K binary bits to encode

a chromosome. And quantum computer will use register of K qubits to present all the possible states (possible points in the feasible region of the optimization problem). The initial mixed state (chromosome will have the same probability in a mixed state) is

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} |j\rangle$$

In this case all points in the feasible region of the optimization problem are involved in the initial state. We can define a Hermitian Hamiltonian H as Neumann entropy production S and optimizing an objective function as $minS$ [3]. The evaluation of fitness value can be described by the unitary transformation

$$\frac{1}{\sqrt{N}} e^{\imath S} |\psi\rangle$$

where $|\psi\rangle$ is a state that corresponds to a chromosome in the population.The phase will depend as example on the Hamming distance between strings (the large the distance, the larger the phase [32]. The selection process can be carried out by applying the unitary transformation $e^{\imath St}$ to the registers. Thus the emulation of GA on a quantum computer realize the quantum soft computing. With a series of applications of this unitary transformation, the solution will have the highest probability according to the principles of GA and of the minimum entropy production [3, 32].

6 Conclusions

Main problems of quantum computing and quantum fast searching algorithms are discussed. The power of quantum computing as massive quantum parallelism can be used to solve the optimization problems in micro control of micro-and nano-robots. Quantum soft computing based on GA and quantum searching algorithms is a new tool for the R&D the flexible structure of quantum intelligent control algorithms.

References

[1] J. Preskill. Quantum Information and Computation.// *http://www.theory.caltech.edu/people/preskill/ph229/* Caltech, 1997.

[2] C.P. Williams and S.H. Clearwater. Explorations in Quantum Computing. Springer-Verlag, N.Y., 1998.

[3] B. Petrov, G. Ulanov, I. Goldenblat and S.V. Ulyanov. Advanced Control of Quantum and Relativistic Dynamic Systems : Physical and Information Aspects, (in Russian). Moscow, Nauka Publ., 1982

[4] T.P. Spiller. Quantum information processing: cryptography, computation and teleportation. Proc. IEEE, vol. 84, 1996, pp.1719-1946.

[5] A. Ekert and R.Jozsa. Quantum computation and Shor's factoring algorithm. *Rev. Modern Phys.*, vol. 68, 1996, pp.733-768.

[6] R.Jozsa. Quantum algorithms and the Fourier transform. *Proc. R. Soc. Lond.*, vol. 454, 1998, pp. 323-337.

[7] E.Bernstein and U.Vazirani. Quantum complexity theory. *SIAM Computing.*, vol. 26, No 5, 1997, pp. 1411-1473.

[8] L.M.Adleman, J. Demarrais and M.-D.A.Huang. Quantum computability. *Proc. R. Soc. Lond.*, vol. A 454, 1998, pp. 339-354.

[9] R. Cleve, A. Ekert, C. Macchiavello and M. Mosca. Quantum algorithm revisited. *Proc. R. Soc. Lond.*, vol. A 454, 1998, pp. 339-354.

[10] V. Vedral, A. Barenco and A. Ekert. Quantum networks for elementary arithmetic operations. *Rep. Prog. Phys.*, vol. A 54, No 1, 1996, pp. 147-153..

[11] A. Steane. Quantum computing. *Rep. Prog. Phys.*, Vol. 61, 1998, pp. 117-173.

[12] M.A. Nielsen, C.M. Caves, B. Schumacher and H. Barnum. Information-theoretic approach to quantum correction and reversible measurement. *Proc. R. Soc. Lond.*, vol. 454A, 1998, pp. 277-304.

[13] C.H.Bennett, P.Cacs, M.Li, P.M.B.Vitanyi and W.Zurek. Thermodynamics of computation and information distance. *Proc. 28-th Annual ACM Symp. Theory of Computing.*, California, May 16-18, 1993, pp. 21-30.

[14] W.H. Zurek. Thermodynamic cost of computation, algorithmic complexity and the information metric. *Nature*, vol. 341, 1989, pp. 311-326.

[15] C.H.Bennett. The thermodynamics of computation: A review. *Int. J. Theoret. Physics*, vol.21, 1982, pp. 905-940.

[16] W.H.Zurek. Algorithmic randomness and physical entropy. *Phys. Rev.*, vol. A 40, 1989, pp. 4731-4751

[17] S. Lloyd. Quantum-mechanical Maxwell's demon. *Phys. Rev.*,vol. A 56, No 5, 1997, pp. 3374-3381.

[18] R. Landauer. Energy needed to send a bit. *Phys. Rev.*, vol. A 217, 1996, pp. 188-193

[19] R. Landauer. The physical nature of information. *Phys. Lett.*, vol. A 217, 1996, pp. 188-193.

[20] R. Landauer. Minimal energy requirements in communicationautomata. *Science*, vol. 272, 1996, pp. 1914-1918.

[21] J.D. Bekenstein. Communication and energy. *Phys. Rev.* vol. D 37, No 9, 1988, pp. 3437-3448.

[22] L.K. Grover A fast quantum mechanical algorithm for database search. *Proc. 35-th Annual ACM on the Theory of Computing*, Pennsylvania, May 22-24, 1996, pp. 212-219

[23] L.K. Grover Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.*, vol. 80, 1998, pp. 2473-2476.

[24] I.L.Chuang, N.Gershenfeld and M.Kubinec. Experimental implementation of fast quantum searching *Phys. Rev. Lett.*,vol. 80, 1998, pp. 3408-3411.

[25] T.Hogg. Highly structured searches with quantum computers. *Phys. Rev. Lett.*,vol. 80, 1998, pp. 2473-2476.

[26] P.W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantun computer. *SIAM J. Comput.*, vol. 26, No 5, 1997, pp. 1484-1509.

[27] M. Bayer, G. Brassard, P.Hoyer and A.Tapp. Tight bounds on quantum searching. *Fortschritte der Physik*, vol.46, No 4/5, 1998, pp. 493- 505.

[28] C.H. Bennet, E. Bernshtein, C. Brassard and U. Vazirani. Strengths and weakness of quantum computing. *SIAM Computing*, vol. 26, No 5, 1997, pp. 1510-1523.

[29] K.M.Obeland and A.M. Despain. Simulating the effect of decoherence and inaccuracies on a quantum computer. *quant-ph/9804038*,16 Apr-1998.

[30] R. Beals, H. Buhrman, R. Cleve and M. Mosca. Quantum lower bounds by polynomials. *quant- ph/9802049*, v3. 30 Sep. 1998.

[31] Y.Ge, L.T. Watson and E.G. Collins. Genetic algorithms for optimization on a quantum computer. *Proc.*1^{st} *Intern. Conference on Unconventional Models of Computation (UMC'98), Springer-Verlag*, Singapore, 1998, pp.218-227.

[32] S..Ulyanov, I. Kurawaki , F. Arai, T. Fukuda, K.Yamafuji and G.G. Rizzotto. Physical limits and information bounds of micro control. Part 1. *Proc. of Intern. Symp. on Micromechatronics and Human Science (MHS'97)*, Nagoya,1997,pp.149-154