Self-Organization Principle and Robust Wise Control Design based on Quantum Fuzzy Inference

Sergey V. Ulyanov [1], Ludmila V. Litvintseva [1] and Sergey S. Ulyanov [2]

[1]YAMAHA Motor Europe N.V. R&D Office, Crema (CR), Italy; [2] MCG "Quantum", Moscow, Russia
ulyanov@yamaha-crema.it

Abstract - This report presents a generalized design strategy of intelligent robust control systems based on quantum/soft computing technologies that enhance robustness of fuzzy controllers by supplying its a self-organizing capability. It is demonstrated that fuzzy controllers prepared to maintain control objects in the prescribed conditions are often fail to control when such a conditions are dramatically changed. We propose the solution of such kind of problems by introducing a generalization of strategies in fuzzy inference from a set of pre-defined fuzzy controllers by a new Quantum Fuzzy Inference based systems. We stress our attention on the robustness features of intelligent control systems. Benchmark simulations of robust intelligent control based on a new Quantum Fuzzy Inference for globally unstable essentially non-linear dynamic system are considered. Based on the simulation results with Quantum Fuzzy Inference a new design principle "*Simple wise control of complex control objects*" is introduced and demonstrated.

Keywords: Robust Wise Control, Self-Organization Principle, Quantum Fuzzy Inference, Quantum Soft Computing

1. Introduction

For complex, essentially non-linear and ill-defined structure dynamic systems that are not easily controlled by traditional control systems (such as P- [I]-D-controllers) - especially in the presence of different stochastic noises - the soft computing methodology provides fuzzy controllers (FC) as one of the alternative way of control system's design [1]. Fuzzy controllers demonstrate their great applicability in cases when control object is ill-defined or it operates under unknown conditions, when traditional (negative feedback-based) controller is failing [1, 2]. Soft computing methodologies, such as genetic algorithms (GA) and fuzzy neural networks (FNN) had expanded application areas of FC by adding learning and adaptation features. But still now it is difficult to design "good" and robust intelligent control system, when its operational conditions have to evolve dramatically (aging, sensor failure, sensor's noises or delay and so on). Such conditions could be predicted from one hand, but it is difficult to cover such situations by a single FC.

One of the solutions seems obvious by preparation of a separate set of knowledge bases (KB-FC) for fixed conditions of control situations, but the following question raises:

Q: *How to judge which KB-FC should be operational in the concrete time moment*?

At this moment the most important decision is a selection of the generalization strategy which will switch the flow of control signals from different FC, and if necessary will modify their output to fit present control object conditions. For this purpose the simplest way is to use a kind of *weighted aggregation of outputs* of each independent FC, but this solution will fail and distribution of weighting factors should be somehow dynamically decided (see below and [1, 2]).

We propose a solution of such kind of generalization problems by introducing a self-organized design process of KB-FC that supported by the *Quantum Fuzzy Inference* (QFI) based on Quantum Soft Computing [3, 4] and Engineering Cybernetics (self-organization) ideas. Proposed QFI system consists of a few KB-FC's (multiple-KB), each of which is prepared for appropriate conditions of control object and excitations by Soft Computing Optimizer. QFI system is a quantum algorithm block, which performs post-processing of the results of fuzzy inference of each independent FC and produces the generalized control signal output. In this case the on-line output of QFI is an optimal robust control

signal, which combines best features of the each independent FC outputs (self-organization principle). Therefore the operation area of such a control system can be expanded greatly as well as its robustness. Robustness of control signal is the background for support the reliability of control accuracy in uncertainty environments.
In this report we give a brief introduction on soft computing tools for designing independent FC and then we will provide QFI methodology, and the simulation example of robust intelligent control based on QFI. Using the simulation results with QFI a new design principle "*Simple wise control of complex control objects*" is illustrated.

2. Problem's formulation

Main problem in modern FC design is how to design and introduce robust KB's into control system for increasing self-learning, self-adaptation and self-organizing capabilities, which enhance robustness of developed FC. Figure 1 shows the interrelations between control quality measures and types of the computational intelligence tools.

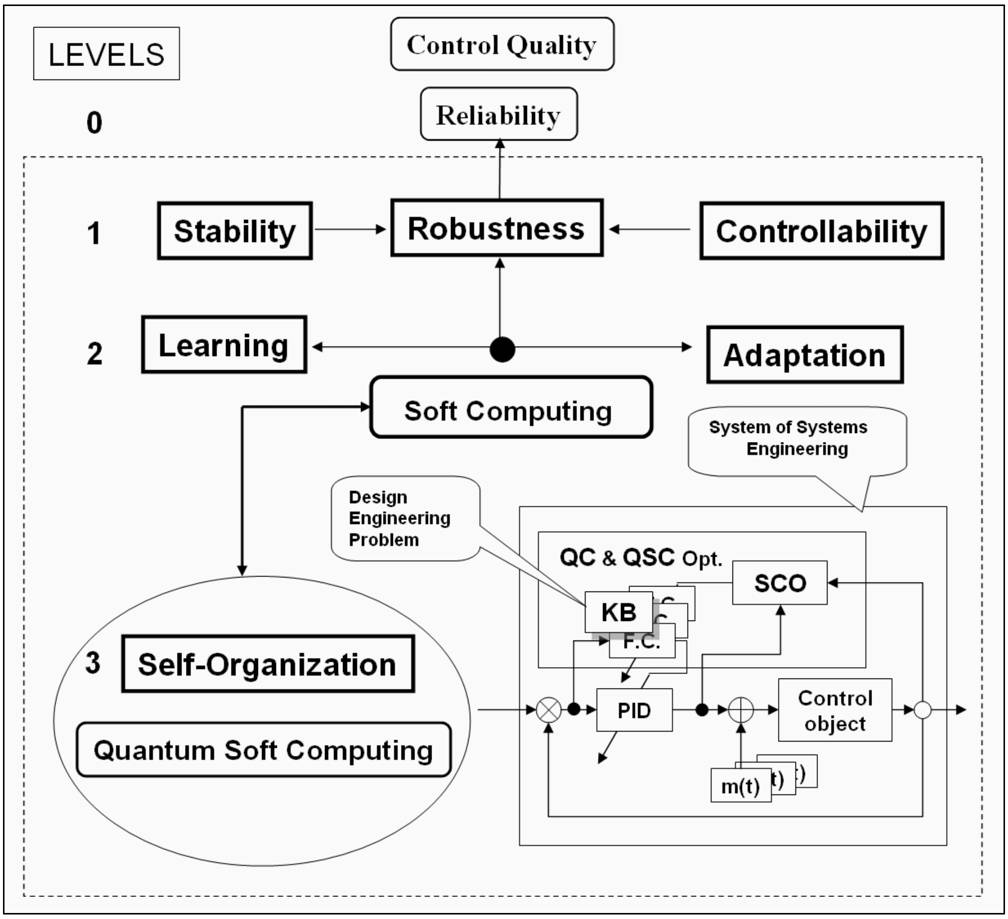


Figure1: *Interrelations between control quality criteria and computational intelligence levels*

Interrelations between stability, controllability and robustness (Level 1 of Figure 1) are studied in [1] and included in software of Soft Computing Optimizer [2].
Remark. The *learning* and *adaptation* aspects of FC's have always the interesting topic in advanced control theory and system of systems engineering. Many learning schemes were based on the back-propagation (BP) algorithm and its modifications (see, for example, [1] and their references).

Adaptation processes are based on iterative stochastic algorithms. These ideas are successfully working if we perform our control task without a presence of ill-defined stochastic noises in environment or without a presence of unknown noises in sensors systems and control loops, and so on. For more complicated control situations learning and adaptation methods based on BP-algorithms or iterative stochastic algorithms do not guarantee the *required* robustness and accuracy of control. The solution of this problem based on Soft Computing Optimizer (SCO) was developed in [1].
For achieving of self-organization (see, Figure 1, Level 3) in intelligent control system it is necessary to use QFI [3, 8]. The described below self-organizing FC design method is based on special form of QFI that uses a few of partial KB's designed by SCO [1, 2].
QFI uses the laws of quantum computing [3-6, 8] as unitary reversible operators and explores three main unitary operations: (i) superposition; (ii) entanglement (quantum correlations or quantum oracle); and (iii) interference. The general structure of QFI block is shown in Figure 2.

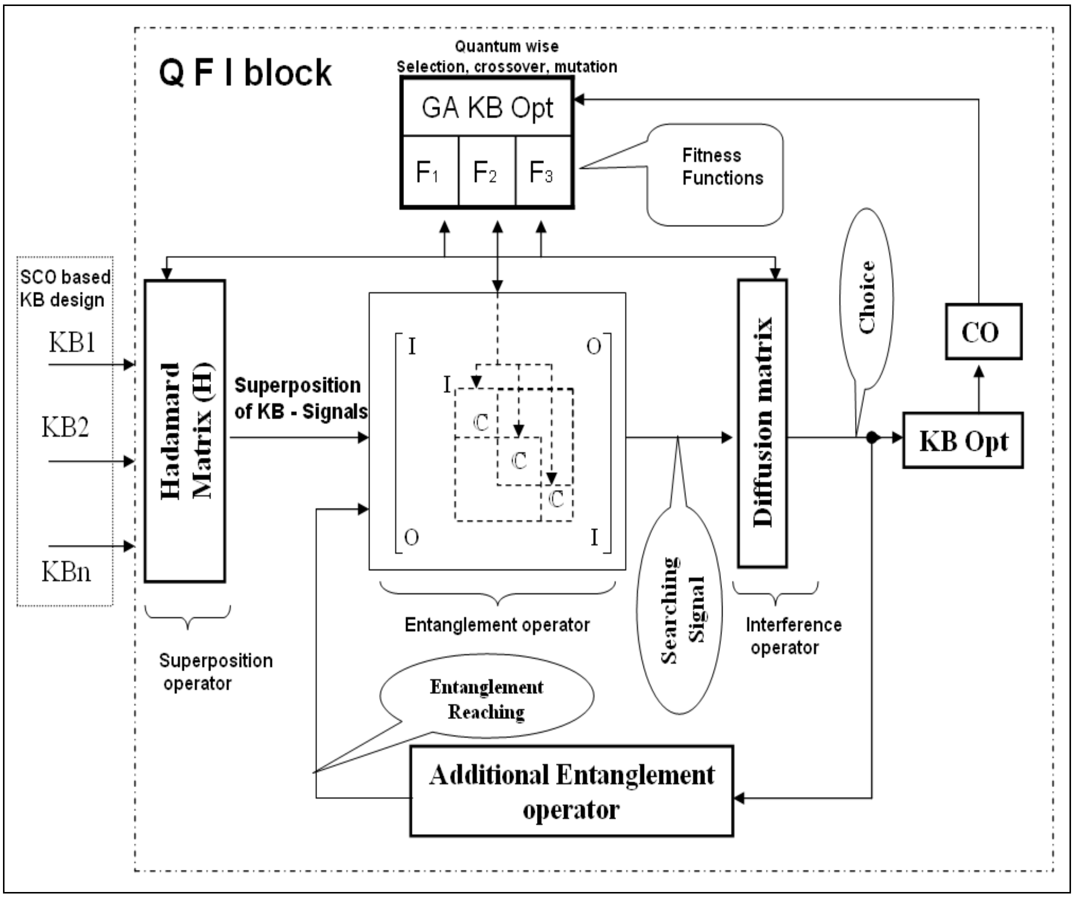


Figure 2: *The structure of QFI block*

According to quantum gate computation [4-9], the logical union of a few KB's in one generalized space is realized with superposition operator; with entanglement operator (that can be described by different models of quantum oracle [8-14]) a search of "successful" marked solution is formalized; and with interference operator together with classical measurement operations we can extract "good" solutions. Additional operator in local feedback plays the role of entanglement reaching for control search of successful result.
<u>Related works</u>: *Quantum (-inspired) genetic algorithms and quantum evolutionary programming*. The so-called generalization of evolutionary algorithms (EA) is Quantum Evolutionary Programming

(QEP), which has two major sub-areas: (i) Quantum-Inspired Genetic Algorithms (QIGA's); and (ii) Quantum Genetic Algorithms (QGA's). The former adopts qubit chromosomes as representations and employs quantum gates for the search of the best solution. The latter tries to solve a key question in this field: what GA's will look like as an implementation on quantum hardware tool. An important point for QGA's is to build a quantum algorithm that takes advantage both - GA's and quantum computing parallelism - as well as true randomness provided by quantum computing. For the interested reader, different models of QEP such as quantum particle swap optimization algorithm and so on have been developed in [3, 7, 8, 15-45]. And some of these models are described briefly below in Appendix 1. The difference and common parts as parallelism of both GA's and quantum algorithms are also compared. The quantum genetic search algorithm in Figure 2 is the generalization form of these QEP's models [3, 8].

The main technical purpose of QFI is to supply in on-line a self-organization capability for many (sometimes unpredicted) control situations based on a few KBs. QFI produces robust optimal control signal for the current control situation using the extraction of a new hidden quantum information from KB 's superposition, reducing procedure and compression of redundant classical information in KB's of individual FCs. Process of rejection and compression of redundant information in classical KB's uses the laws of quantum information theory [5, 8]. Specifically, we employ an efficient algorithm for data compression that gathers entropy across a number of qubits into a small subset of highly random qubits. Decreasing of redundant classical information in control laws of KB-FC increases the robustness of control processes without loss of important control quality such as the reliability of control accuracy (see, Figure 1). As a result, a few KB-FC with QFI can be adapted in on-line to unexpected change of external environments and to uncertainty in initial information.

We introduce main ideas of quantum computation and quantum information theory applied in developed QFI methods. QFI-ideas are also introduced. Robustness of new types of self-organized intelligent control systems for global unstable essentially non-linear control object is demonstrated. Using the simulation results with QFI a new design principle "*Simple wise control of complex control objects*" is demonstrated.

3. QFI model based on quantum computing

In this report we introduce briefly the necessary particularities of quantum computing and quantum information theory that are used in the quantum block (see, Figure 2) supporting a self-organizing capability of FC. Additional facts about quantum correlation and quantum information theory are described in Appendices 2 and 3.

3.1 *Main structures of Quantum computing*. For design of QFI based on a few KB's it is needed to apply the additional operations to partial KB's output's signals that drawing and aggregate the value information from different KB's. Soft computing tool does not contain corresponding necessary operations [3, 7, 8]. The necessary unitary reversible operations are called superposition, entanglement (quantum correlation) and interference those are mathematical operators of quantum computing [3 - 6]. Naturally (see, Appendix 1) two problems in quantum computing are discussed: (1) Given a set of functional points $S = \{(x, y)\}$ find the operator U such that $y = U \cdot x$; (2) Given a problem, to find the quantum circuit that solves it. Algorithms for solving these problems may be implemented in a hardware quantum gate or in software as computer programs running on a classical computer [4, 8]. It is shown [4 - 6, 8] that in quantum computing the construction of a universal quantum simulator based on classical effective simulation is possible. The fundamental result of quantum computation stays that all of the computation can be embedded in a circuit, which nodes are the universal gates. These gates offer an expansion of unitary operator U that evolves the system in order to perform some computation. In general form [5 - 8], quantum computing model consists of five steps: (i) an initial quantum state; (ii) application of Hadamard's transforms to initial state for preparation of superposition state; (iii) oracle application operator to superposed state (entanglement operator); (iv) application of interference operator; and (v) a measurement of result. It is assumed that certain computational problems can be solved on a quantum computer with a lower complexity than on classical computers since there are problems, which are efficiently solvable by quantum algorithms but not classically up to now. In doing so, quantum algorithms take advantage of basic computational techniques, namely superpositioning, quantum parallelism, and quantum interference. Additionally, entanglement seems to be source of computational power quantum algorithms can benefit from. Quantum states are compounded by means of the tensor (Kronecker) product of the basic state spaces. Such a combination is referred to as the quantum register. It appears that the speed-up in quantum computation is due to the entanglement, by which many computations are performed in parallel. In that sense, entanglement is a special new resource in quantum computing. From functionality point of view quantum algorithms are classified on two groups: (i) decision-making algorithms; and (ii) search algorithms. When describing quantum computation, we are interested in the properties exhibited by specific states and the changes induced by applying some operations. For this case, algebraic formalism can be applied that supports abstractions for reasoning about quantum effects and indicates important quantum properties explicitly rather than focusing solely on describing a physical system. In this case quantum algebra has several attractive properties including an explicit representation of important quantum properties, mechanism for compact describing and efficient reasoning about large numbers of bits in a highly entangled state, and a descriptive representation of quantum operations. It is hardware independent and can be used as a notation for quantum computation or as the basis for a programming language [8, 15 - 21].

Remark. It remains extremely difficult to reason about quantum effects and to develop quantum algorithms. Quantum computation has different concerns, and in addition, it involves the manipulation of distinctly unfamiliar properties like entanglement, phase, and superposition. These two properties as superposition and entanglement have no classical analog and provide part of the power of quantum computation. Phase has traditionally been treated as continuous, but a basic unit of phase simplifies reasoning without sacrificing expressiveness. Representations of quantum operations indicate that the searching properties of functions must be introduced into the input of quantum gate [8].

The segmental actions of the quantum gate and of measurement make up a quantum block (see, Figure 2). The quantum block is repeated *k* times in order to produce a collection of *k* basis vectors. Since measurement is a non-deterministic operation, these basis vectors will not necessarily be identical, and each basis vector encodes a peace of the information needed to solve the problem. The last part of the algorithm involves interpretation of the collected basis vectors in order to get the final answer for the initial problem with some probability. The fundamental result of quantum computation stays that all of the computation can be embedded in a circuit, who's nodes are the universal gates. These gates offer an expansion of unitary operator U that evolves the system in order to perform some computation. It is shown that in quantum computing the construction of a universal quantum simulator based on classical effective simulation is possible [4, 5]. Hence, a quantum gate approach can be used in a global optimization of Knowledge Base (KB) structures of intelligent control systems that are based on quantum computing, on a quantum genetic search algorithm (QGSA) [8, 15, 16, 22 - 31] and quantum learning processes [3, 7, 8, 48].

3.2 *Quantum information resources in QFI algorithm*. The algorithm for coding, searching and extracting the value information from two KB's of fuzzy PID controllers designed by SCO is described in [49]. Optimal drawing process of value information from a few KB's that are designed by soft computing is based on the following four facts from quantum information theory [5, 8]: (i) the effective quantum data compression; (ii) the splitting of classical and quantum parts of information in quantum state; (iii) the total correlations in quantum state are "mixture" of classical and quantum correlations; and (iv) the exiting of hidden (locking) classical correlation in quantum state [50]. The QFI algorithm uses these four facts from quantum information theory: (i) compression of classical

information by coding in computational basis $\{|0\rangle,|1\rangle\}$ and forming quantum correlation between different computational bases (Fact 1); (ii) separating and splitting total information and correlations on "classical" and "quantum" parts using Hadamard transform (Facts 2 and 3); (iii) extract unlocking information and residual redundant information by measuring the classical correlation in quantum state (Fact 4) using criteria of maximal corresponding probability amplitude. These facts are the informational resources of QFI background. Using them it is possible to extract additional amount of quantum value information from smart KB's produced by SCO to design a wise control using compression and rejection procedures of the redundant information in a classical control signal.
Below we discuss the application of this algorithm in QFI structure.

4. Design of self-organizing fuzzy controllers based on QFI

The kernel of the abovementioned FC design tools is a so-called SC Optimizer implementing advanced soft computing ideas. SCO is considered as a new flexible tool for design of optimal structure and robust KB's of FC based on a chain of genetic algorithms (GA's) with information-thermodynamic criteria for KB optimization and advanced error back-propagation algorithm for KB refinement. Input to SCO can be some measured or simulated data (called as 'teaching signal" (TS)) about the modelling system. For TS design (or for GA fitness evaluation) we use stochastic simulation system based on the control object model. More detail description of SCO is given in [1, 2].
Figure 3 illustrates as an example structure and main ideas of self-organized control system consisting of two FC's coupling in one QFI chain that supplies a self-organizing capability.

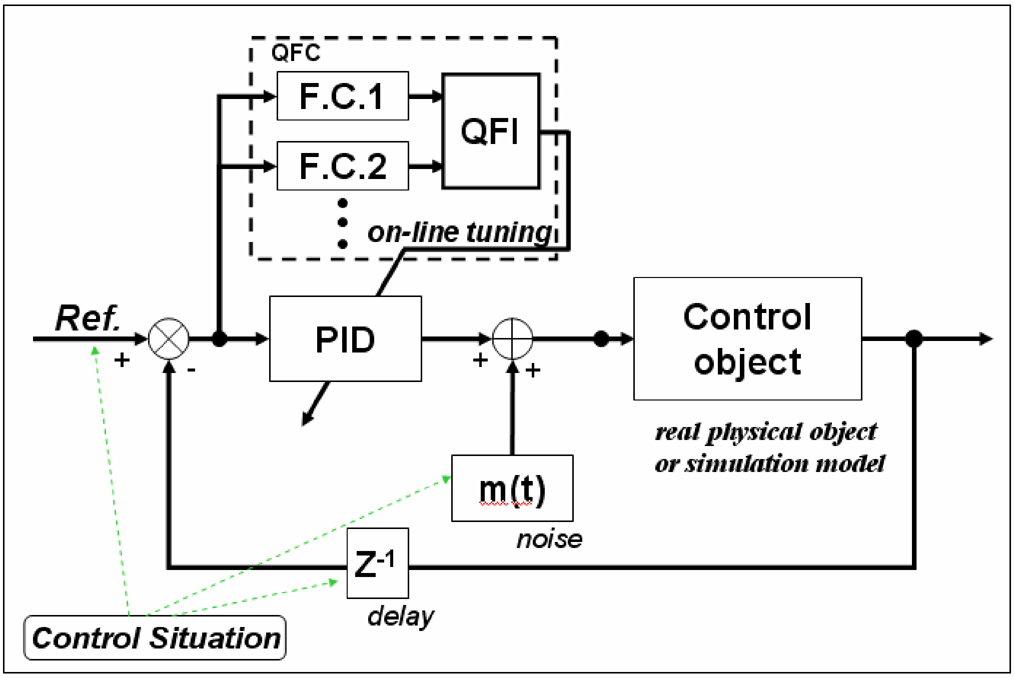


Figure 3: *Main structure of intelligent self-organized control system*

As above mentioned, QFI block (see, Figure 2) is based on three main quantum operators of quantum computing: superposition of classical states, entanglement, interference, and classical measurement. The input to the QFI block is considered as a superposed quantum state $K_1(t)\otimes K_2(t)$, where $\otimes$ is tensor product operation; and $K_{1,2}(t)$ are the outputs PID gain coefficients from fuzzy controllers FC1 and FC2 designed by SCO for the given control task in different control situations (for example, in the presence of different stochastic noises). The algorithm of superposition calculation is described in [8, 49]. Using the abovementioned four facts from quantum information theory QFI extracts the value information from KB1 and KB2. In this case between KB1 and KB2 (from quantum information theory point of view) we organize a communication channel using quantum correlations that is impossible in classical communication theory [8]. We discuss for simplicity the situation in which an arbitrary amount of correlation is unlocked with a one-way message [50] (see, in details Appendix 3).

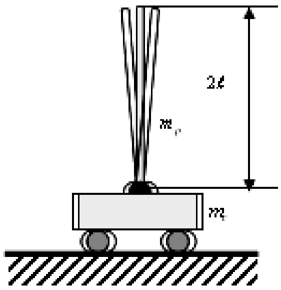
Example. Let us consider the communication process between two KB's as communication between two players *A* and *B*, and let $d = 2^n$. According to the law of quantum mechanics, initially we must prepare a quantum state description by density matrix ρ from two classical states (KB1 and KB2). The initial state ρ is shared between subsystems held by *A* (KB1) and *B* (KB2), with respective dimensions *d*, $\rho = \frac{1}{2d}\sum_{k=0}^{d-1}\sum_{t=0}^{1}\left(|k\rangle\langle k| \otimes |t\rangle\langle t|\right)_A \otimes \left(U_t |k\rangle\langle k| U_t^{\dagger}\right)_B$. Here $U_0 = I$ and U_1 changes the computational basis to a conjugate basis: $\left|\langle i\,|U_1|\,k\rangle\right| = 1/\sqrt{d} \quad \forall\, i,k$. In this case, *B* chooses $|k\rangle$ randomly from d states in two possible random bases, while *A* has complete knowledge on his state. The state ρ can arise from the following scenario. *A* picks a random *n*-bit string k and sends B $|k\rangle$ or $H^{\otimes n}|k\rangle$ depending on whether the random bit *t* =0 or 1. Here *H* is the Hadamard transform. *A* can send *t* to *B* to unlock the correlation later. Experimentally, the Hadamard transform and measurement on single qubits are sufficient to prepare the state ρ and later extract the unlocked correlation in ρ'. The initial correlation is small, $I_{Cl}^{(l)}(\rho) = \frac{1}{2}\log d$. The final amount of information after the complete measurement M_A in one-way communication is as $I_{Cl}(\rho') = I_{Cl}^{(l)}(\rho) = \log d + 1$, i.e., the amount of accessible information increase. This phenomenon is impossible classically. However, states exhibiting this behaviour need not be entangled and corresponding communication can be organized using Hadamard's transform [50]. Therefore, using the Hadamard's transformation and a quantum correlation as communication between a few KB's it is possible to increase initial information by quantum correlation.

In present report we consider a simplified case of QFI from Figure 2, when with the Hadamard transform is organized an unlocked correlation in superposition of two KB's; the entanglement operation is modelled as quantum oracle that can estimates a maximum of amplitude probability in corresponding superposition of classical states. Interference operator extracts this maximum of amplitudes probability with a classical measurement. Below we discuss application of described QFI model to control non-linear globally unstable dynamic system.

5. Benchmark simulations of cart-pole system

The cart-pole dynamic system is well-known Benchmark in intelligent control problem and described by 2 *nd* order differential equations for calculating the force to be used for moving the cart and shown in Figure 4. In above equations, *g* is the acceleration due to gravity (usually $9.8\, m/\sec^2$), m_c is the mass of the cart, *m* is the mass of the pendulum, *l* is the half-length of the pendulum, *z* is a cart position, *u* is an applied force in Newtons and $\xi(t)$ is a stochastic excitation with an appropriate probability density function. Consider excited motion of the given dynamic system under fuzzy PID-control. Let the system be disturbed by different stochastic noises. Stochastic simulation of random excitations with appropriate probability density functions is based on nonlinear forming filters methodology developed in [1]. Our control goal is to balance the pole in vertical position ($\theta = 0$) with limited cart's position and velocity.

According to general structure of intelligent self-organized control system (see, Figure 3) let us design the following two fuzzy controllers.



$$\ddot{\theta} = \frac{g\sin\theta + \cos\theta\left(\frac{(u+\xi(t)) + \{+a_1\dot{z} + a_3 z\} - ml\dot{\theta}^2\sin\theta}{m_c + m}\right) - k\dot{\theta}}{l\left(\frac{4}{3} - \frac{m\cos^2\theta}{m_c + m}\right)}$$

$$\ddot{z} = \frac{u + \xi(t) + \{-a_1\dot{z} - a_3 z\} + ml(\dot{\theta}^2\sin\theta - \ddot{\theta}\cos\theta)}{m_c + m}$$

Figure 4: *Cart-pole dynamic system: model and equations of motion*

FC1-design: *Teaching situation* 1. The following model parameters: $[m_c, m, l, k, a_1, a_3] = [1, 0.1, 0.5, 0.4, 0.1, 5]$ and initial conditions $[\theta_0, \dot{\theta}_0, z_0, \dot{z}_0] = [10, 0.1, 0, 0]$ are considered. Stochastic excitation is a Gaussian noise (symmetric probability density function). PID controller *K*-gains ranging area is [0,100]. Delay time in sensor system is 0.001.

FC2 design: *Teaching situation* 2. Model parameters and initial conditions are the same as in teaching *Situation* 1. Stochastic excitation is a Rayleigh noise (un-symmetric probability density function). *K*-gains ranging area is [0,100]. Delay time in sensor system is 0.001.

By using SC Optimizer and teaching signal (TS) obtained by the stochastic simulation system with GA [1, 2]) or from experimental data, we design KB1 and KB2 of FC1 and FC2, which optimally approximate the given TS (from viewpoint of the chosen fitness function). When KB1 and KB2 are designed, we can organize QFI based on outputs of FC1 and FC2 as shown in Figure 3. We considered different control situations and compared control performances of FC1, FC2 and self-organized control system based on QFI with two FC's.

In Table 1 five different control situations are described. Stochastic noises in given situations are shown in Figure 5.

Table 1: *Types of control situations*

Teaching situations (S1, S2)

Unknown situations (S3, S4, S5)

	Noise			delay		Initial cond
	type	max				[θ δθ/δτ]
S1	Gaussian1	3		0.001		[10 0.1]
S2	Rayleigh 1	4		0.001		[10 0.1]
S3	Rayleigh 2	4		0.001		[10 0.1]
S4	Uniform	3		0.001		[10 0.1]
S5	Gaussian2	3		0.008		[10 0.1]

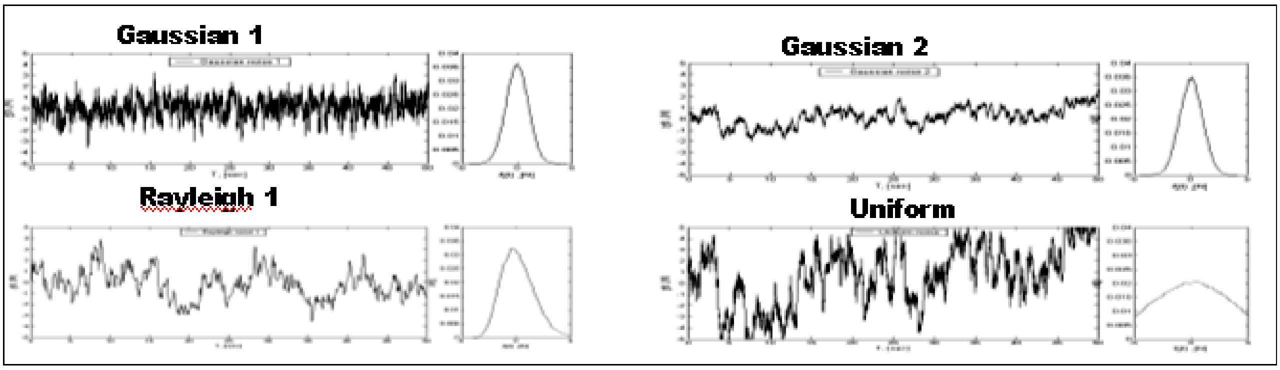


Figure 5: *Types of stochastic noises*

Figures 6 - 8 show cart-pole dynamic motion and control laws of PID controller under different types of control, where WFC is a weighted control (output PID-gains calculated as average from outputs of FC1 and FC2), QFC is a quantum fuzzy controller based on QFI.
The Figure 9 shows the total performance level comparison in different control situation (the situation S4 is one of examples). The simulation results are shown that in unknown situations (for example in the case of *S4* situation shown in figures) WFC, FC1 and FC2 are loose robustness, but using self-organization ability QFC shows a stable control.

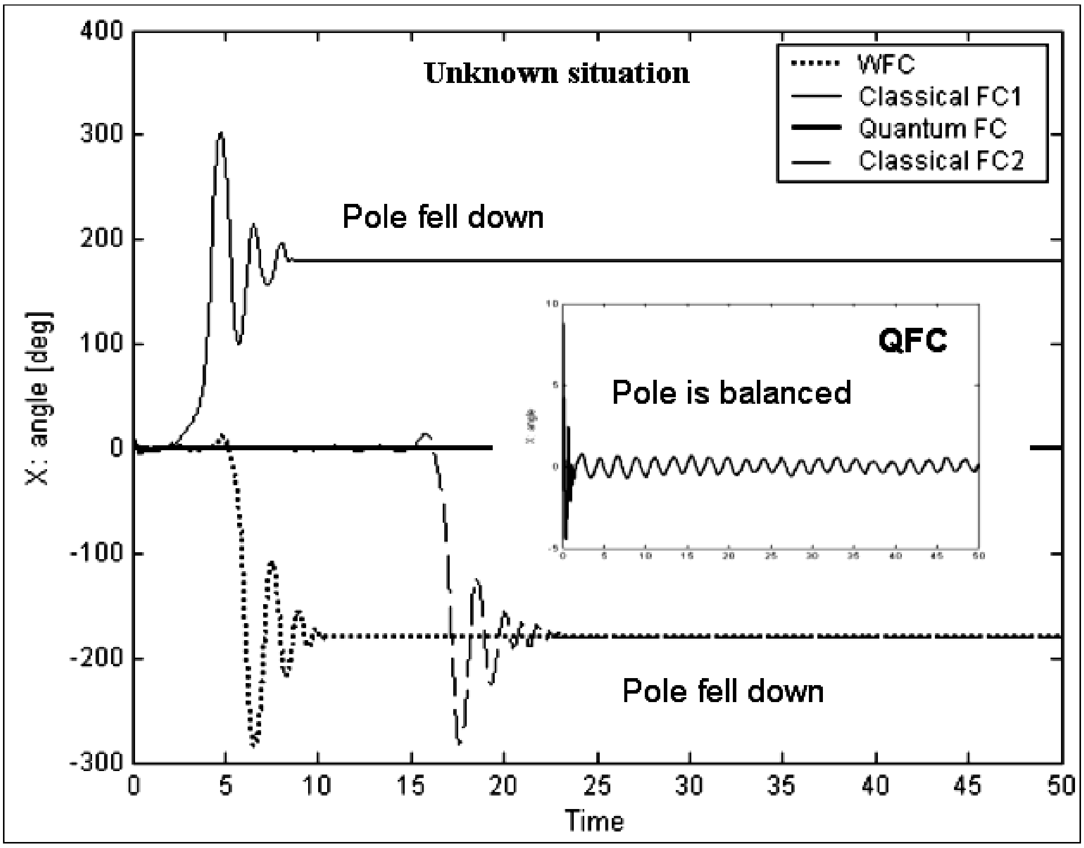


Figure 6: *Cart-Pole system - Unknown situation S4.*
Pole dynamic motion under different types of control

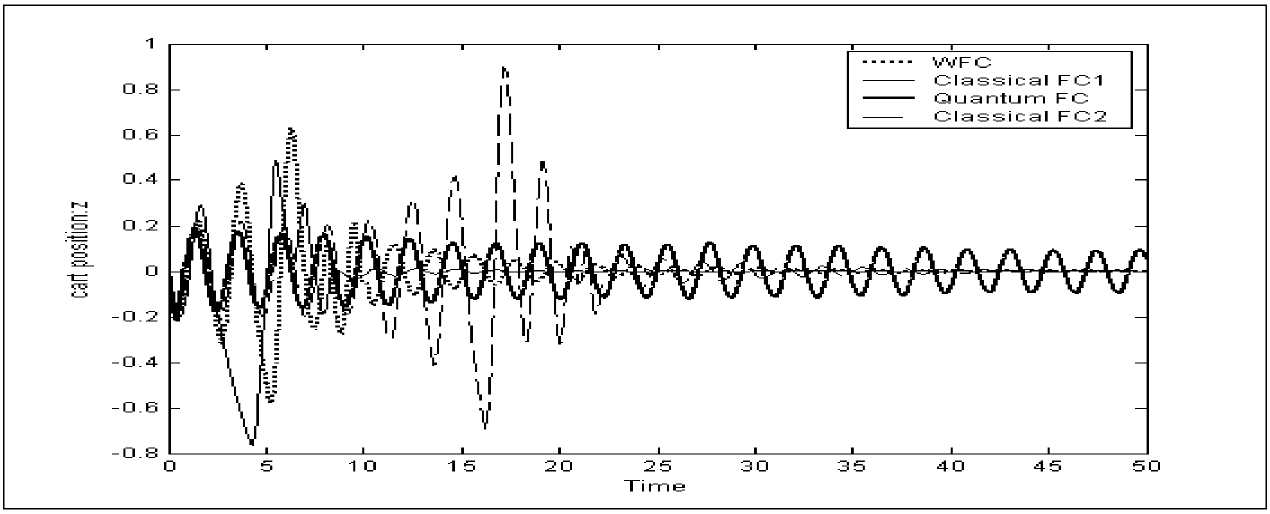


Figure 7: *Cart-Pole system - Unknown situation S4. Cart dynamic motion under different types of control*

Simulation results show that using quantum strategies with QFI is possible to organize the optimal robust control signal from two KBs outputs with simple control laws of PID coefficients gains. From quantum game theory point of view we have the demo of *Parrondo paradox* without using an entanglement: from two classical KBs that are not winner in different environments using quantum strategy we can design with QFI one winner control signal. This effect was described also in [49, 51]. Thus, the considered Benchmark shows the effectiveness of quantum computing application for solution of classical problems in intelligent fuzzy control.

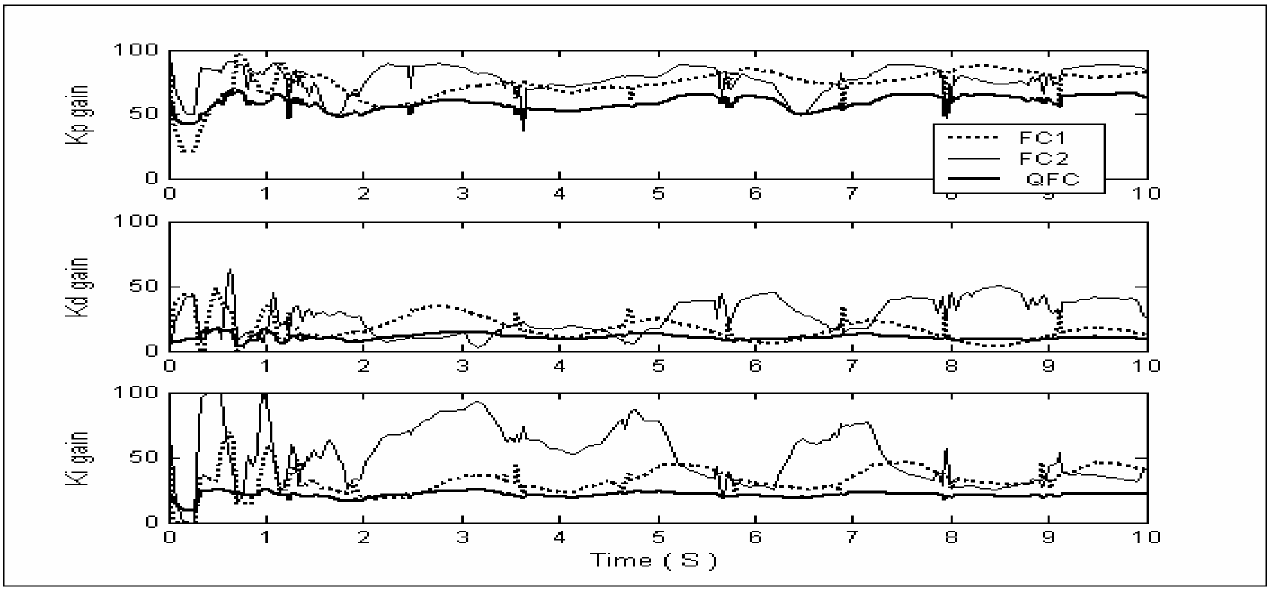


Figure 8: *Cart-Pole system - Unknown situation S4. PID-*control laws

Related works. Another approach to design of fuzzy control based on quantum computing model is considered in [52 - 55]. Quantum computing model without entanglement is considered in [56].

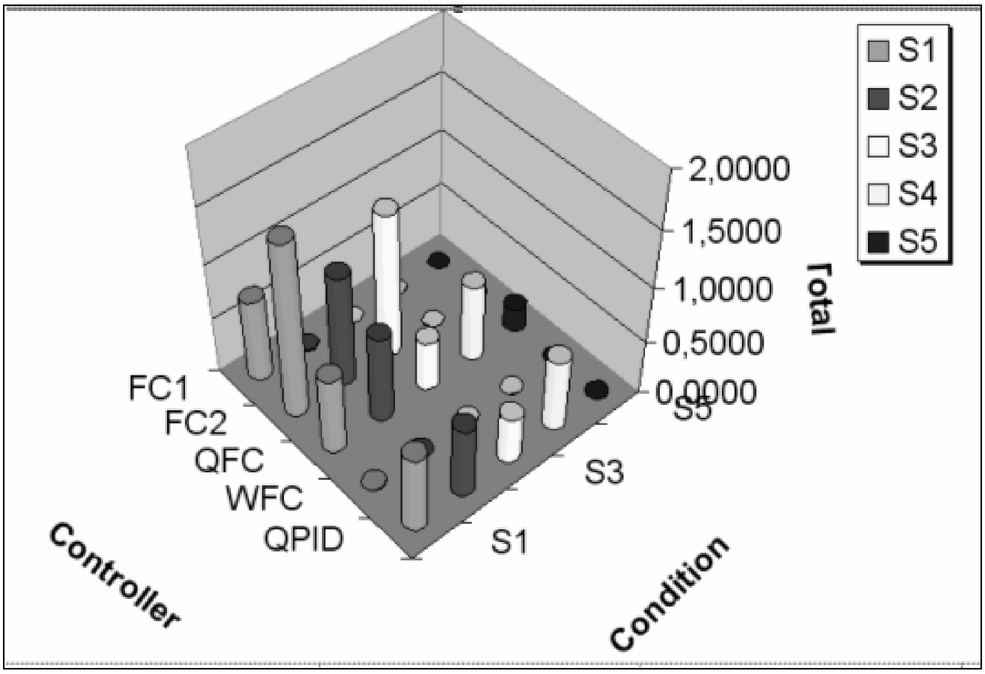


Figure 9: *Cart-Pole system. Total performance level comparison*

7. Conclusions

1. SCO allows us to model different versions of KB's of FC that guarantee robustness for fixed control environments.
2. The QFI block enhances robustness of fuzzy controllers using a self-organizing capability.
3. Designed FC based on QFI achieves the prescribed control objectives in many control situations.
4. Using SCO and QFI we can design wise control of essentially non-linear stable and, especially of unstable dynamic systems, in the presence of uncertainty in initial information about external excitations and in presence of changing reference signals (control goal), and model parameters.
5. QFI based FC requires minimum of initial information about external environments and an internal structure of control object.

References

[1] L.V. Litvintseva, S.V. Ulyanov, K. Takahashi, S.A. Panfilov, I.S. Ulyanov and S.S. Ulyanov, "Intelligent Robust Control Design based on New Types of Computation," Vol. 60, **Note del Polo** (Ricerca), Universita degli Studi di Milano, 134 p., 2004

[2] S.A. Panfilov, L.V. Litvintseva, I.S. Ulyanov, K. Takahashi, S.V. Ulyanov, A.V. Yazenin and T. Hagiwara, "Soft computing optimiser for intelligent control systems design: the structure and applications," **J. Systemics, Cybernetics and Informatics,** Vol. 1, No 5, pp.1 –6, 2003

[3] S.V. Ulyanov, "Quantum Soft Computing in control process design: Quantum Genetic Algorithms and Quantum Neural Networks approaches", In: **Proc. WAC**'2004, *Conf. ISSI*, Seville, Spain, June 28-July 1, 2004

[4] US Patent No 6,578,018B1, "System and method for control using quantum soft computing" (Inventor: S.V. Ulyanov), Date of Patent: July 10, 2003

[5] M.A. Nielsen and I.L. Chuang, "Quantum Computation and Quantum Information," **Cambridge Univ. Press**, UK, 2000; M.L. Dalla Chiara and R. Guintitni, "Reasoning in quantum theory: Sharp and unsharp quantum logic," **Kluwer Academic Publ**., 295 p., 2004

[6] D.C. Marinescu and G.M. Marinescu, "Approaching quantum computing," **Pearson Prentice Hall**, New Jersey, USA, 386 p., 2005

[7] S.V. Ulyanov, K. Takahashi et al, “Quantum Soft Computing: Quantum Global Optimisation and Quantum Learning Processes - Benchmarks of Applications in AI, Informatics, and Intelligent Control Systems”, In: **Proc. SCI**’2003, Vol. III, USA, Orlando, July 27-30, pp. 422 - 427, 2003
[8] S.V. Ulyanov, “Quantum information and quantum computational intelligence: Backgrounds and applied tools of intelligent computational technologies. Pts 1, 2, 3” Vol. 73, **Note del Polo** (Ricerca), Universita degli Studi di Milano, 2005 (in print)
[9] F. Ghisi and S.V. Ulyanov, “The information role of entanglement and interference in Shor quantum algorithm gate dynamics,” **J. Modern Optics**, Vol. 47, No 12, pp. 2079 – 290, 2000
[10] E. Kashefi, A. Kent, V. Vedral and K. Banaszek, “Comparison of quantum oracles,” **Physical Review**, Vol. **A**65, No 5, pp. 050304-1 - 050304-4, 2002
[11] A.J. Bessen, “The power of various real-valued quantum queries,” **J. of Complexity**, Vol. 20, No 5, pp. 699 – 712, 2004
[12] A. Atici, “Comparative computational strength of quantum oracles,“ **arXiv**: quant-ph/0312107v1, 11 Dec 2003, 23 p.
[13] H. Azuma, “A quantum algorithm for examining oracles,“ **arXiv**: quant-ph/0408013v1, 3 Aug 2004, 19 p.
[14] K. Iwama, A. Kawachi, R. Raymond and Sh. Yamashita, “Robust quantum algorithms for oracle identification,“ **arXiv**: quant-ph/0411204 v1, 30 Nov 2004, 19 p.
[15] A. Leier, “Evolution of quantum algorithms using genetic programming,“ **PhD Thesis**, Dortmund, 2004, 199 pp
[16] L. Spector, “Automatic quantum computer programming: A genetic programming approach,” Kluwer Academic Publ., 2004
[17] A. van Tonder, “A lambda calculus for quantum computation,” **SIAM J. of Computing**, Vol. 33, No 5, pp. 1109 – 1135, 2004
[18] S. Bettelli, T. Calarco and L. Serafini, “Toward an architecture for quantum programming,” **Eur. Phys. J**. Vol. **D**25, pp. 181 – 200, 2003
[19] A. Klappenecker and M. Rotteler, “Quantum software reusability,” **Intern. J. Foundations of Computer Sciences**, Vol. 14, No 5, pp. 777 – 796, 2003
[20] P. Selinger, “Towards a quantum programming language,“ **Math Structures Comp Sciences**, Vol. 14, No 4, pp. 527 – 586, 2004; T. Altenkirch, J. Grattage, J.K. Vizzotto and A. Sabry, “An algebra of pure quantum programming,“ **arXiv**: quant-ph/0506012v1, 1 Jun 2005, 21 p.
[21] M. Sauerhoff and D. Sieling, “Quantum branching programs and space-bounded non-uniform quantum complexity,“ **Theoretical Computer Sciences**, Vol. 334, pp. 177 – 225, 2005
[22] Sh. Yang, M. Wang and L. Jiao, “A novel quantum evolutionary algorithm and its application,“ In: **Proc. IEEE Congress on Evolutionary Computation** (*CEC*’2004), June 19 – 23, 2004, Vol. 1, pp. 820 – 826, 2004; “A quantum particle swarm optimisation,“ *ibid*, pp. 320 – 324; “The quantum evolutionary programming,“ In: **Proc. 5th Intern. Confer. Computational Intelligence and Multimedia Applications** (*ICCIMA*’03), IEEE Computer Society, 2003
[23] J. Sun, B. Feng and W. Xu, “”Quantum swarm optimisation with particles having quantum behaviour,“ In: **Proc. IEEE Congress on Evolutionary Computation** (*CEC*’2004), June 19 – 23, 2004, Vol. 1, pp. 325 – 331, 2004
[24] G. Zhang, W. Jin and L. Xu, “A novel parallel quantum genetic algorithm,” In: **Proc. 4th IEEE Intern. Conf. Parallel and Distributed Computing: Applications and Technologies** (*PDCAT*’2003), 27 – 29 Aug 2003, pp. 693 – 697, 2003
[25] G.A. Giraldi, R. Portugal and R.N. Thess, “Genetic algorithms and quantum computation,” **arXiv**: cs. NE/0403003v1, 4Mar 2004
[26] K.-H. Han and J.-H. Kim, “Quantum-inspired evolutionary algorithms with a new termination criterion, H_ε gate, and two-phase scheme,” **IEEE Transactions on Evolutionary Computation**, Vol. 8, No 2, pp. 156 - 169, 2004
[30] Y. Li, Y. Zhang, R. Zhao and L. Jiao, “The immune quantum-inspired evolutionary algorithm,” In: **IEEE Intern. Conf. Systems, Man and Cybernetics**, 10 – 13 Oct, 2004, Vol. 4, pp. 3301 – 3305, 2004
[31] M. Lukac, M. Perkowski, H. Goi et all, “Evolutionary approach to quantum and reversible circuits synthesis,” **Artificial Intelligence Review**, Vol. 20, pp. 361 –417, 2003; A. Singh, L.M. Bharadwaj and S.

Harpreet, “DNA and quantum based algorithms for VLSI circuits testing,“ **Natural Computing**, Vol. 4, No 1, pp. 53 – 72, 2005
[32] S.P. Ghoshal, “Optimizations of PID gains by particle swarm optimisations in fuzzy based automatic generation control,” **Electric Power Research**, Vol. 72, No 3, pp. 203 – 212, 2004
[33] Z.-L. Gaing, “A particle swarm optimisation approach for optimum design of PID controller in AVR system,“ **IEEE Trans. Energy Conversion**, Vol. !9, No 2, pp. 384 – 391, 2004
[34] Y. Liu, J. Zhang and Sh. Wang, “Optimization design based on PSO algorithm for PID controller,” In: **Proc. 5th Word Congress on Intelligent Control and Automation**, June 15 – 19, 2004, Hangzhou, P.R. China, pp. 2419 –242, 2004
[35] M.-P. Song and G.-Ch. Gu, “Research on particle swarm optimisation: A review,” In: **Proc. 3rd Intern. Conf. Machine Learning and Cybernetics**, Shanghai, 26 – 29 Aug, 2004, Vol. 1, pp. 2236 – 2241, 2004
[36] K.E. Parsopoulos and M.N. Vrahatis, “Recent approaches to global optimisation problems through Particle Swarm Optimization,” **Natural Computing**, Vol. 1, No 2, pp. 235 – 306, 2002
[37] J. Vesterstrom and R. Thomsen, “A comparative study of differential evolution, particle swarm optimization, and evolutionary algorithms on numerical Benchmark problems,” In: **Proc. IEEE Congress on Evolutionary Computation** (*CEC*’2004), June 19 – 23, 2004, Vol. 2, pp. 1380 – 1387, 2004
[38] O. Hrstka, A. Kucerovà, M. Leps and J. Zeman, “A competitive comparison of different types of evolutionary algorithms,” **Computers and Structures**, Vol. 81, No 11, pp. 1979 – 1990, 2003
[39] S. Kukkonen and J. Lampinen, “Comparison of generalized differential evolution to other multi-objective evolutionary algorithms,” In: **Proc. European Congress on Computational Methods in Applied Sciences and Engineering** (*ECCOMAS*’2004), Juvaskyla, 24 – 28 July, 2004, pp. 1 – 20, 2004
[40] H. Schmidt and G. Thierauf, “A combined heuristic optimisation technique,” **Advanced in Engineering Software**, Vol. 36, No 1, pp. 11 – 19, 2005; Y. Jin and J. Branke, “Evolutionary optimisation in uncertain environments - A survey,” **IEEE Transactions Evolutionary Computation**, Vol. 9, No 3, pp. 303 – 317, 2005
[41] X.H. Shi, Y.C. Liang, H.P. Lee, C. Lu and L.M. Wang, “An improved GA and a novel PSO-GA-based hybrid algorithm,” **Information Processing Letters**, Vol. 93, No 5, pp. 255 – 261, 2005
[42] Y. Da and G. Xiurun, “An improved PSO-based ANN with simulated annealing technique,” **Neurocomputing**, Vol. 63, No 1, pp. 527 – 533, 2005; B. Lu, L. Wang, Y.-H. Jin, F. Tang and D.-X. Huang, “Improved particle swarm optimisation combined with chaos,” **Chaos, Solitons and Fractals**, Vol. 25, No 5, pp. 1261 – 1271, 2005
[43] R. Mendes, J. Kennedy and J. Neves, “The fully informed particle swarm: Simpler, maybe better,” **IEEE Trans. Evolutionary Computation**, Vol. 8, No 3, pp. 204 – 210, 2004
[44] S.A. Panfilov, S.V. Ulyanov, L.V. Litvintseva and A.V. Yazenin, “Fast algorithm for efficient simulation of quantum algorithm gates on classical computer,“ **J. Systemics, Cybernetics and Informatics,** Vol. 2, No 3, pp. 1 –6, 2004
[45] Z. Zilic and K. Radecka, “The role of super-fast transforms in speeding up quantum computations,” In: **Proc. 32nd IEEE Intern. Symp. Multiple-Valued Logic** (ISMVL’02), 15 – 18 May, 2002, pp. 129 - 135, 2002; “FPGA emulation of quantum circuits,” In: **Proc. IEEE Intern. Confer. Computer Design**: *VLSI in Computers and Processors* (ICCD’04), 11 – 13 Oct., 2004, pp. 310 – 315, 2004
[46] A. Maitra and P. Parashar, “Hadamard type operations for qubits,“ **arXiv**: quant-ph/0505068v1, 10 May 2005, 8 p.
[47] S. Aaronson, “Quantum computing and hidden variables,” **Physical Review**, Vol. **A**71, No 3, pp. 032325-1 – 032325-16, 2005
[48] R.A. Servedio and S.J. Gortler, “Equivalence and separations between quantum and classical learnability,” **SIAM J. of Computing**, Vol. 33, No 5, pp. 1067 - 1092, 2004
[49] S.V. Ulyanov, K. Takahashi, S.A. Panfilov, L.V. Litvintseva et all, “Quantum soft computing via robust control: Classical efficient simulation of wise quantum control in non-linear dynamic systems based on quantum game gates,” In: **Proc. of ICSCCW**’2003, Antalya, Turkey, pp. 11 - 41, September 9 - 11, 2003
[50] D.P. DiVincenzo, M. Horodecki, D.W. Leung, J.A. Smolin and B.M. Terhal, “Locking classical correlation in quantum states,” **Physical Review Letters**, Vol. 92, No 6, pp. 067902, 2004
[51] S.V. Ulyanov, L.V. Litvintseva, S.S. Ulyanov and A.L. Panfilov, “Computational intelligence with quantum game’s approach and robust decision-making in communication information uncertainty,” In: **Proc.**

Intern. Conference on Computational Intelligence (ICCI'2004), Nicosia, North East University, North Cyprus, May 27 – 29, pp. 172 – 186, 2004
[52] G.R. Rigatos and S.G. Tzafestas, "Parallelization of a fuzzy control algorithm using quantum computation," **IEEE Transactions on Fuzzy Systems,** Vol. 10, No 4, pp. 451 - 460, 2002
[53] V. Kreinovich and L. Longprè, "Fast quantum algorithms for handling probabilistic and interval uncertainty," **Math Log Quart**, Vol. 50, No 4, pp. 405 -416, 2004
[54] **US Patent** No 6,675,154 B2, "Method and system for the quantum mechanical representation and processing of fuzzy information," (Inventor: G.S. Jaeger), Date of Patent: Jan. 6, 2004
[55] N. Kouda, N. Matsui and H. Nishimura, "Control for swing-up of an inverted pendulum using qubit neural network," In: **Proc. SCIE**'02 Aug 5-7, 2002, Osaka, Japan, pp. 765 – 770, 2002
[56] E. Biham, G. Brassard, D. Kenisberg and T. Mor, "Quantum computing without entanglement," **Theoretical Computer Science**, Vol. 320, No 1, pp. 15 – 33, 2004

Appendix 1: *Evolutionary programming and quantum computing models*. Evolutionary algorithm (EA) is an effective algorithm, which simulates the natural evolution. The best-known examples are as following: (i) genetic algorithm (GA); (ii) evolutionary programming (EP); and (iii) evolutionary strategy (ES); (iv) particle swarm optimisation (PSO); (v) differential evolution optimization (DEO) etc.

The so-called generalization of EA is Quantum Evolutionary Programming and has two major sub-areas: (i) Quantum-Inspired Genetic Algorithms (QIGAs); and (ii) Quantum Genetic Algorithms (QGAs). The former adopts qubit chromosomes as representations and employs quantum gates for the search of the best solution. The latter tries to solve a key question in this field: what GAs will look like as an implementation on quantum hardware. An important point for QGAs is to build a quantum algorithm that takes advantage both - GA's and quantum computing parallelism - as well as true randomness provided by quantum computing. Different model generalizations of EA on quantum strategies application are described in [15, 22 - 31]. Below the difference and common parts as parallelism of both GA's and quantum algorithms are compared.

A1.1. *Genetic/Evolutionary computation and programming*. Evolutionary computation is a kind of self-organization and self-adaptive intelligent technique which analogies the process a natural evolution. According to Darwinism and Mendelism, it is through the reproduction, mutation, selection and competition that the evolution of life is fulfilled. Simply stated, GA's are stochastic search algorithms based on the mechanics of natural selection and natural genetics. GA's applied to its capabilities for searching large and non-linear spaces where traditional methods are not efficient or also attracted by their capabilities for searching a solution in non-usual spaces such as for learning of quantum operators and in design of quantum circuits [15, 16, 31]. An important point for GA's design is to build an algorithm that takes advantage of computing parallelism. But as to huge and complex systems, especially to the nonlinear systems, the traditional GA also has shortcomings such as huge calculating storage, losing of the best chromosomes, less guarantee for converging to the whole optimal result earlier.

Remark: *PSO and DEO models*. PSO is an evolutionary computation technique developed by Eberhart and Kennedy (1995), which inspired by social behavior of bind flocking and fish schooling. It is some-like GA for it also begins with random population and searches for optima by updating the population, while PSO has no evolution operators such as crossover and mutation. In PSO, the potential solutions, called particles, "flown" through the whole space by following the current optimum particles. Each particle keeps track of the best solution it has experienced so far (pbest). The other "best" solution being tracked is the best individual in a particle's neighbors (lbest). When a particle takes all the individuals as its topological neighbors, then the best value is a global best (gbest). Each particle changes its velocity toward the "pbest" and "lbest" components at each iteration. Acceleration is weighted by a random number toward "pbest" and "lbest" locations. Applications of PSO technique to design of optimal PID coefficient gains are described in [32 - 34]. The DEO was introduced by Storn and Price in 1995. It resembles the structure of an EA, but differs from traditional EA's in its generation of new candidate solutions and by its use of a "greedy" selection scheme. These algorithms can use a floating-point representation for the solutions in the population. Thus, the evolutionary operators are completely different from those used in methods known as GA's, ES's and EP. A competitive comparison of different types of evolutionary algorithms is discussed in [37 - 42].

Remark: *About parallel GA's models*. There exist some problems in the initialization of GA's that they can be very demanding in terms of computation and memory, and sequential GA's may get trapped in a sub-optimal region of the search space thus becoming unable to find better quality solutions. So, parallel genetic algorithms (PGA's) are proposed to solve more difficult problems, which need large population. PGA's are parallel implementation of GA's, which can provide considerable gains in terms of performance and scalability. The most important advantage of PGA's is that in many cases they provide better performance than single population-based algorithms, even when the parallelism is simulated on conventional computers. PGA's are not only an extension of the traditional GA sequential model, but they represent a new class of algorithms in that they search the space of solutions differently.

Existing parallel implementations of GA's can be classified into three main types of PGA's: (i) Global single-population master-slave GA's; (ii) Massive parallel GA's; and (iii) Distributed GA's. Global single-population master-slave GA's explores the search space exactly as a sequential GA and are easy to implement and significant performance improvements are possible in many cases. Massive parallel GA's are also called fine-grained PGA's and they are suited for massively parallel computers. Distributed GA's are also called coarse-grained PGA's or island-based GA and are the most popular parallel methods because of its little communication overhead and its diversification of the population.

EA is such a random searching algorithm based on the above model. It is origin of the GA that is derived from machine learning, ES, which is brought forward in numerical optimization, and EP.

Remark. EP is an efficient algorithm in solving optimization problems, but the criterion EP is of torpid convergence. Compared with GA, EP has some difference in characteristics. *First*, the evolution of GA is on the locus of chromosome, while EP directly operates on the population's behavior. *Second*, GA is based on the Darwinism and genetics, so the crossover is the major operator. EP stresses on the evolution species, so there are not operations directly on the gene such as crossover, and mutation is the only operator to generate new individuals. Thus mutation is the only operator in EP and consequently it is the breakthrough point of EP. Cauchuy-mutation and logarithm-normal distribution mutation algorithms are examples, which also improved the performance of EP. *Third*, there is transformation of genotype and phenotype in GA, which does not in EP. *Fourth*, the evolution of EP is smooth and the evolution is much steady than GA, however it relies much on its initial distribution. From the evolution mechanism, the EP that adopts Gauss mutation to generate offspring is characteristics of a slow convergent speed. Therefore, finding more efficient algorithm too speed up the convergence and improve the quantity of solution has become an important subject in the research of EP.

A1.2. *Quantum computing*. The fundamental result of quantum computation stay that all the computation can be can be expanded in a circuit, which nodes are the universal gates and in quantum computing universal quantum simulator is possible. These gates offer an expansion of unitary operator U that evolves the system in order to perform some computation. Thus, naturally two problems are discussed: (1) Given a set of functional points $S = \{(x, y)\}$ find the operator U such that $y = U \cdot x$; (2) Given a problem, to find the quantum circuit that solves it. The former can be formulated in the context of GA's for learning algorithms while the latter through evolutionary strategies. Quantum computing has a feature called quantum parallelism that cannot be replaced by classical computation without an exponential slowdown. This unique feature turns out to be the key to most successful quantum algorithms. Quantum parallelism refers to the process of evaluating a function once a superposition of all possible inputs to produce a superposition of all possible outputs. This means that all possible outputs are computed in the time required to calculate just one output with a classical computation. Superposition enables a quantum register to store exponentially more data than a classical register of the same size. Whereas a classical register with N bits can store one value out 2^N, a quantum register can be in a superposition of all 2^N values. An operation applied to the classical register produces one result. An operation applied to the quantum register produces a superposition of all possible results. This is what is meant by the term "*quantum parallelism*."

Remark. Unfortunately, all of these outputs cannot be as easily obtained. Once a measurement is taken, the superposition collapses. Consequently, the promise of massive parallelism is offset by the inability to take advantage of it. This situation can be changed with the application hybrid algorithm (one part is Quantum Turing Machine (QTM) and another part is classical Turing Machine) as in Shor's quantum factoring algorithm that took advantage of quantum parallelism by using a quantum Fourier transform. A new type of algorithm has been devised, herein referred as QGA (Quantum Genetic Algorithm), which is substantially a merging of a genetic algorithm and a quantum algorithm (see, Figure 2). QGA (as the component of general Quantum

Evolutionary Programming) starts from this idea, which can take advantage of both quantum computing and GA's paradigms.

The key of this general idea is to explore the quantum effects of superposition and entanglement operators to create a generalized coherent state with the increased diversity of quantum population that store individuals and their fitness of successful solutions. Using the complementarity between entanglement and interference operators with a quantum searching process (based on interference and measurement operators) successful solutions from designed state can be extracted. In particularity, especially the major advantage for a QGA consists in using of the increased diversity of a quantum population (due to superposition of possible solutions) in optimal searching of successful solutions in non-linear stochastic optimization problem for control objects with uncertainty/fuzzy dynamic behavior.

It has been found a method of performing a quantum algorithm. The main difference of this method with the well known quantum algorithms consists in that the superposition, entanglement and interference operators are determined for performing selection, crossover and mutation operations according to a genetic algorithm. Moreover, entanglement vectors, generated by the entanglement operator of the quantum algorithm, may be processed by a wise controller implementing GA, before being input to the interference operator. This algorithm of the invention may be easily implemented in a hardware quantum gate or with a software computer program running on a computer. Moreover, it can be used in a method for controlling a process and a relative control device of a process which is more robust, required minimum of initial information about dynamic behavior of control objects in design process of intelligent control system, or random noise insensitive (invariant) in measurement system and in control feedback loop [3, 4, 49].

A1.3. *Quantum genetic algorithm models*. Another innovative aspect of this approach consists in a method of performing a genetic algorithm, wherein the selection, crossover and mutation operations are performed by means of the quantum algorithm. Also a method of designing quantum gates is provided. This method provides a standard procedure to be followed for designing quantum gates. By following this procedures it is easy to understand how basic gates, such as the well-known two-qubits gates for performing a Hadamard rotation or an identity transformation, must be coupled together for realizing a hardware quantum gate performing classically a desired quantum algorithm. The quantum algorithm gates can be used in a quantum computer or a simulation of a quantum computer. A quantum gate is used in a global optimization of Knowledge Base (KB) structures of intelligent control systems that are based on quantum computing and on a quantum genetic search algorithm (QGSA) [49].

This idea sketched out a Quantum Genetic Algorithm (QGA), which takes advantage of both the quantum computing and GA's parallelism. The key idea is to explore the quantum effects of superposition and entanglement to create a physical state that store individuals and their fitness. When measure the fitness, the system collapses to a superposition of states that have that observed fitness. QGA starts from this idea, which can take advantage of both quantum computing and GA's paradigms.

Remark. Again, the difficulty is that a measurement of the quantum result collapses the superposition so that only one result is measured. At this point, it may seem that we have gained little. However, depending upon the function being applied, the superposition of answers may have common features with interference operators. If these features can be ascertained, it may be possible to divine the answer searching for probabilistically.

The next key feature to understand is *entanglement*. Entanglement is a quantum (correlation) connection between superimposed states. Entanglement produces a quantum correlation between the original superimposed qubit and the final superimposed answer, so that when the answer is measured, collapsing the superposition into one answer or the other, the original qubit also collapses into the value (0 or 1) that produces the measure answer. In fact, it collapses to all possible values that produce the measured answer. For example, as mentioned above, the key step in QGA is the fitness measurement of a quantum individual. We begin by calculating the fitness of the quantum individual and storing the result in the individual's fitness register. Because each quantum individual is a superposition of classical individuals, each with a potentially different fitness, the result of this calculation is a superposition of the fitnesses of the classical individuals. This calculation is made in such a way as to produce an entanglement between the register holding the individual and the register holding the fitness(es). *Interference* operation is used after entanglement operator for extraction of successful solutions from superposed outputs of quantum algorithms.

The well-known complementarity or duality of particle and wave is one of the deeps concepts in quantum mechanics. A similar complementarity exists between entanglement and interference. The entanglement measure is a decreasing function of the visibility of interference.

Let us consider the complementarity in a simple two-qubit pure state case.

<u>*Example*</u>: *Complementarity of entanglement and interference*. Consider the entangled state $|\psi\rangle = a|0_1\rangle|0_2\rangle + b|1_1\rangle|1_2\rangle$ with the constraint of unitarity: $a^2 + b^2 = 1$. Then make a unitary transformation with rotation gate in first basis $\{|0_1\rangle, |1_1\rangle\}$ on the first qubit, $|0_1\rangle \to \cos\alpha|0_1\rangle + \sin\alpha|1_1\rangle$, and obtain $|\psi\rangle \to |\psi'\rangle = a\left(\cos\alpha|0_1\rangle + \sin\alpha|1_1\rangle\right)|0_2\rangle + b\left(\cos\alpha|1_1\rangle - \sin\alpha|0_1\rangle\right)|1_2\rangle$. Finally observe the first qubit without caring about the second one. The probability to get the state $|0_1\rangle$ is $P_{|0_1\rangle} = \frac{1}{2}\left[1 + \left(a^2 - b^2\right)\cos 2\alpha\right]$, which is a typical interference pattern if we regard the angle α as a control parameter. The visibility of the interference is: $\Gamma \equiv \left|a^2 - b^2\right|$ which vanishes when the initial state is maximally entangled, i.e., $a^2 = b^2$, while it becomes maximum when the state is separable, i.e. $a = 0$ or $b = 0$. On the other hand the entanglement measure is partially traced von Neumann entropy as follows:

$$E \equiv S\left(\rho_{red}\right) = -a^2 \log a^2 - b^2 \log b^2,$$

where the reduced density operator: $\rho_{red} = Tr_2|\psi'\rangle\langle\psi'| = Tr_2|\psi\rangle\langle\psi| = a^2|0_1\rangle\langle 0_1| + b^2|1_1\rangle\langle 1_1|$.

The entanglement takes the maximum value $E = 1$ when $a^2 = b^2$ and the minimum value $E = 0$ for $a = 0$ or $b = 0$. Thus the more the state is entangled, the less visibility of the interference and vice versa. Another popular measure of entanglement such as the negativity may be better for a quick illustration. The negativity is minus twice of the least eigenvalue of the partial transpose of the density matrix. In this case, it is $N = 2|ab|$. The complementarity is for this case as following: $N^2 + \Gamma^2 = 1$. This constraint between the entanglement and the interference comes from the condition of unitarity: $a^2 + b^2 = 1$.

Thus, in quantum algorithms these measures of entanglement and interference are not independent and the efficiency simulation of success solutions of quantum algorithms is correlated with equilibrium interrelations between these measures. Similar to classical GA in QGA allows the use of any fitness function that can be calculated on a QTM (Quantum Turing machine) without collapsing a superposition, which is generally a simple requirement to meet.

The QGA differs from classical GA in that each individual is a *quantum* individual. In classical GA when selecting an individual to perform crossover, or mutation, exactly one individual is selected. This is true regardless of whether there are other individuals with the same fitness. This is not the case with a quantum algorithm. By selecting an individual, all individuals with the same fitness are selected. In effect, this means that a single quantum individual in reality represents multiple classical individuals.

Thus, in QGA each quantum individual is a superposition of one or more classical individuals. To do this several sets of quantum registers are used. Each individual uses two registers: (1) the *individual* register; and (2) the *fitness* register. The first register stores the superimposed classical individuals. The second register stores the quantum individual's fitness. At different times during the QGA the fitness register will hold a single fitness value (or a quantum superposition of fitness values). A population will be N of these quantum individuals.

According to the law of quantum mechanics the effect of the fitness measurement is a collapse and this process reduces each quantum individual to a superposition of classical individuals with a common fitness. It is the key step in the QGA. Then the crossover and mutation operations would be applied. The more significant advantage of QGA's will be an increase in the production of good building blocks (same as schemata in classical GA's) because, during the crossover, the building block is crossed with a superposition of many individuals instead of with only one in classical GA's. To improve the convergence we need also better evolutionary (crossover/mutation) strategies. The evolutionary strategies are efficient to get closer the solution but not to complete the learning process that can be realized efficiently with quantum fuzzy neural network (QFNN) [3, 7, 8].

Remark. This approach based on the concept and principles of quantum computing, quantum genetic algorithms and parallel quantum genetic algorithm can be used to solve combinatorial optimization problems and much better results can be achieved than conventional GA's. In order to introduce the strong parallelism of quantum computing into general continuous function optimization problems, the diffusion between models of parallel GA's and QGA's can be used as example, for a novel parallel evolutionary algorithm called coarse-grained parallel evolutionary genetic algorithm. The main idea of this novel algorithm is that the strategies of updating quantum gate using qubit phase comparison method and adjusting search grid adaptively, and extend version of coarse-grained model called hierarchical ring model.

A1.4. *Quantum algorithm gates and quantum programming*. The background of this and similar approaches consists in corresponding quantum algorithm gate (QAG) design that described in [4, 5, 8]. The general structure of the QAG is based on three quantum operators (superposition, entanglement, and interference) and measurement. The QAG acts on an initial canonical basis vector to generate a complex linear combination (called a superposition) of basis vectors as an output. This superposition contains the information to answer the initial problem. After the superposition has been created, entanglement, interference and measurement takes place in order to extract the answer information. In quantum mechanics, a measurement is a non-deterministic operation that produces as output only one of the basis vectors in the entering superposition. The probability of every basis vector of being the output of measurement depends on its complex coefficient (probability amplitude) in the entering complex linear combination. It is relatively easy to develop some set of sound equational principles. Inspired by equivalence on classical computations, one may hypothesise, that certain equations should any simply verify that both sides of the equation have the same denotation. The natural step is to develop reasoning principles on quantum programming language programs (for example, language QML [20]) themselves, which avoid the detour via the denotational semantics. For example, given the following QML definition of the Hadamard gate: $H\,x = \text{if } x \text{ then } \left(\mathit{false} + (-1) * \mathit{true}\right) \text{ else } \left(\mathit{false} + \mathit{true}\right)$. We should like to verify that $H\left(H\,x\right)$ is observationally equivalent to x, using a derivation like:

$$
\begin{aligned}
H\left(H\,x\right) = {} & \text{if } \left(\text{if } x \text{ then } \left(\mathit{false}+(-1)*\mathit{true}\right) \text{ else } \left(\mathit{false}+\mathit{true}\right)\right) \\
& \quad \text{then } \left(\mathit{false}+(-1)*\mathit{true}\right) \\
& \quad \text{else } \left(\mathit{false}+\mathit{true}\right) \\
& \quad \text{-- by commuting conversion for "if"} \\
= {} & \text{if } x \\
& \quad \text{then if } \left(\mathit{false}+(-1)*\mathit{true}\right) \\
& \qquad \text{then } \left(\mathit{false}+(-1)*\mathit{true}\right) \\
& \qquad \text{else } \left(\mathit{false}+\mathit{true}\right) \\
& \quad \text{else if } \left(\mathit{false}+\mathit{true}\right) \\
& \qquad \text{then } \left(\mathit{false}+(-1)*\mathit{true}\right) \\
& \qquad \text{else } \left(\mathit{false}+\mathit{true}\right)
\end{aligned}
$$

$$
\begin{aligned}
& \quad \text{-- by "if"} \\
= {} & \text{if } x \\
& \quad \text{then } \left(\mathit{false} - \mathit{false} + \mathit{true} + \mathit{true}\right) \\
& \quad \text{else } \left(\mathit{false} + \mathit{false} + \mathit{true} - \mathit{true}\right) \\
& \quad \text{-- by simplification and normalisation} \\
= {} & \text{if } x \text{ then } \mathit{true} \text{ else } \mathit{false} \\
& \quad \text{-- by } \eta\text{-rule for "if"} \\
= {} & x
\end{aligned}
$$

A sound and complete equational theory for the functional quantum programming language QML is developed in [20].

Appendix 2: *Quantum information Processing*. Quantum information theory has strict rules on how to extract information out of an unknown quantum state. Optimal drawing process of value information from few KB's that are designed by soft computing is based on following four facts from quantum information theory: (*i*) the effective quantum data compression; (*ii*) the splitting of classical and quantum parts of information in quantum state; (*iii*) the total correlations in quantum state are "mixture" of classical and quantum correlations; and (*iv*) the exiting of hidden (locking) classical correlation in quantum state.

Let us briefly consider the physical meaning of these facts and its role in optimal control signal design.

Fact 1: *Quantum Data Compression*. Shannon has shown how much a message constructed from N independent letters (x_a), where each letter occurs with *a priori* probability p_a, can be compressed. The Shannon entropy H is defined as following: $H(p_a) = -\sum_a p_a \log_2 p_a$. Therefore, a block code of length *NH* bits encodes all typical sequences irrespective of how the atypical sequences are encoded and the probability of error will still be less than ε. In quantum information theory the letters are density matrices and one has to distinguish two cases, namely when the density matrices correspond to ensembles of *q* pure states, $|\phi_a\rangle$, or when they are formed from density matrices ρ_a, with probability p_a. Considering the case of a pure-state ensemble, the density matrix of a message consisting of N letters is $\rho^{(N)} = \rho \otimes \rho \otimes \cdots \otimes \rho$, where $\rho = \sum_a p_a |\phi_a\rangle\langle\phi_a|$, and the von Neumann entropy of the message S is simply related to the entropy of the ensemble, $S(\rho^{(N)}) = NS(\rho)$. It is well known that in general case $H(p) \geq S(\rho)$, i.e. the Shannon entropy is greater then von Neumann entropy [5]. It means that with quantum information approach possible make more deep compression of classical value information.

Fact 2: *Splitting of information in a particular quantum state into classical and quantum part*. Consider performing a general measurement on the state, $A_i A_i^\dagger$, such that $\rho_B^i = \dfrac{A_i \rho_B A_i^\dagger}{Tr(A_i \rho_B A_i^\dagger)}$. The final state of subsystem B is then $\sum_i A_i \rho_B A_i^\dagger = \sum_i p_i \rho_B^i$. The entropy of the residual states is $\sum_i p_i S(\rho_B^i)$. The classical information obtained by measuring outcomes i with probabilities p_i is $H(p)$. If the quantum states ρ_B^i have support of orthogonal subspaces, then the entropy of the final state (after measurement) is the sum of the residual quantum entropy $\sum_i p_i S(\rho_B^i)$ and the classical information, i.e., $S\left(\sum_i p_i \rho_B^i\right) = \underbrace{H(p)}_{Classical} + \underbrace{\sum_i p_i S(\rho_B^i)}_{Quantum}$. We see then that the information in a quantum state may be split into a *quantum* and a *classical* part. Therefore, in our case we produce with SC optimizer a classical part of information and *deficit* of classical information is $\Delta I = S\left(\sum_i p_i \rho_B^i\right) - \underbrace{\sum_i p_i S(\rho_B^i)}_{Quantum} = \underbrace{H(p)}_{Classical}$. It means that it is possible to extract additional amount of quantum value information from smart KB's (produced by SC optimizer) for design wise control using compression procedure with the rejection of the redundant information in classical control signal (using corresponding quantum correlation).

Fact 3: *Total, classical and quantum correlation amounts*. Entanglement, and quantum correlations in general, are typical quantum resources. However, not all correlations have pure quantum nature. Generically, total correlations are "mixture" of classical and quantum correlations. An important issue is to know to what extent classical correlations are used in quantum algorithms. For example, if one is able to determine the classical part of correlations then by the optimal positive operator valued measurement (POVM) one can extract some information in classical form leaving the quantum state with less entropy. The total amount of correlation can be separated on "classical" and "quantum" parts and is equal to the maximal classical/quantum mutual information $I(A:B)$, thus providing it with a direct operational interpretation.

Fact 4: *Hidden (locking) classical correlation in quantum state*. The surprising fact that incremental proportionality for $I_{Cl}(\rho) = \max_{M_A \otimes M_B} I(A:B)$ obtained by local measurements $M_A \otimes M_B$ on the state ρ_{AB} can be violated in some extreme manner for a mixed initial state ρ : a single classical bit, sent from A to B, can result in an arbitrary large increase in $I_{Cl}(\rho)$. This phenomenon can be viewed as a way of locking classical correlation in the quantum state ρ. Since incremental proportionality of $I_{Cl}(\rho)$ holds classically, the phenomenon of locked correlation is purely quantum effect. It is direct consequence of the indistinguishability of non-orthogonal quantum states. Therefore, there exist quantum bipartite states, which contain a large locked classical correlation that is unlocked by a disproportional small amount of classical communication. There are $(2n+1)$-qubit states for which a one-bit message doubles the optimal classical mutual information between measurement results on the subsystems, from $n/2$ bits to n bits. This phenomenon is impossible classically. However, states exhibiting this behavior *need not be entangled* and corresponding communication can be organized using Hadamard's transform [50].

These facts are the informational resources of QFI background. Using these facts it is possible to extract additional amount of quantum value information from smart KB's produced by SC optimizer for design a *wise* control using compression and rejection procedures of the redundant information in a classical control signal.

Figure 2 shows the algorithm for coding, searching and extraction the value information from two KB's that designing by SCO. This algorithm use above mentioned four Facts from quantum information theory: (i) compression of classical information by coding in computational basis $\{|0\rangle, |1\rangle\}$ and forming quantum correlation between different computational bases (Fact 1); (ii) separating and splitting total information on "classical" and "quantum" parts using Hadamard transform (Facts 2 and 3); (iii) extract unlocking information and residual redundant information by measurement the classical correlation in quantum state (Fact 4) using criteria of maximal corresponding amplitude probability. We discuss in Sections 3.3 and 4 the application of this algorithm in QFI structure.

Appendix 3: *Total correlation and hidden (looking) correlation in quantum states*. It is believed that the expected power of a quantum computing is derived from genuine quantum resources. Entanglement, and correlations in general, are typical quantum resources. However, as mentioned above in Appendix 2, not all correlations have pure quantum nature. Generically, total correlations are "mixture" of classical and quantum correlations. An important issue is to know to what extent classical correlations are used in quantum algorithms. For example, if one is able to determine the classical part of correlations then by the optimal measurement one can extract some information in classical form leaving the quantum state with less entropy.

Remark. Physically these quantities can be defined via the amount of work (noise) that is required to erase (destroy) the correlations: for the total correlation, we have to erase completely, for the quantum correlation one has to erase until a separable state is obtained, and the classical correlations the maximal correlation left after erasing the quantum correlation. The total amount of correlations, as measured by the minimal rate of randomness that are required to completely erase all correlations in ρ_{AB} (in many copy scenario), is equal to the quantum mutual information.

A3.1. *Classical and quantum correlation*. The classical mutual information of a quantum state ρ_{AB} can be defined naturally as the maximum classical mutual information that can be obtained by local measurements $M_A \otimes M_B$ on the state ρ_{AB}: $I_{Cl}(\rho) = \max_{M_A \otimes M_B} I(A:B)$. Here $I(A:B)$ is the classical mutual information defined as: $I(A:B) \equiv H(p_A) + H(p_B) - H(p_{AB})$, H is the entropy function, and p_{AB}, p_A, p_B the probability distributions of the joint and individual outcomes of performing the local measurement $M_A \otimes M_B$ on ρ.

<u>Example</u>: *Mutual information and classical correlation*. To understand the role of classical correlation and its compatible with the mutual information, the quantum mutual information is evaluated for an arbitrary bipartite quantum state ρ_{AB} as *Stratonovich*'s amount: $I(A:B) = S(\rho_A) + S(\rho_B) - S(\rho_{AB})$. Consider a system AB in a state ρ_{AB} with probability p to be in a state ρ_A and $(1-p)$ to be in another state ρ_B. For the present state of the system AB the mutual information can be easily calculated to obtain

$$I(A:B) = 2H\left(\frac{1}{2}\left[1+\sqrt{p^2+(1-p)^2}\right]\right) - H\left(\frac{1}{2}\left[1+\sqrt{1+3p^2-3p}\right]\right). \quad \text{(A3.1)}$$

If ρ_{AB} is separable, then its relative entropy of entanglement is zero. Therefore, no measurement can lead to classical correlation that saturates, when added to the relative entropy of entanglement, the mutual information between the two subsystems. This confirms the necessity to use the quantum discord as a quantum counterpart for the classical correlation rather than the relative entropy of entanglement.

The physical relevance of $I_{Cl}(\rho)$ is many-fold: (i) $I_{Cl}(\rho)$ is the maximum classical correlation obtainable from ρ by purely local processing; (ii) $I_{Cl}(\rho)$ corresponds to the classical definition when ρ is "classical," i.e., diagonal in some local product basis and corresponds to a classical distribution; (iii) when ρ is pure, $I_{Cl}(\rho)$ is the correlation defined by the Schmidt basis and thus equal to the entanglement of the pure state; and finally (iv) $I_{Cl}(\rho)=0$ iff $\rho_{AB}=\rho_A\otimes\rho_B$.

Any good correlation measures should satisfy certain axiomatic properties: (i) Correlation is a non-local property and should not increase under local processing (*monotonicity*) (I); (ii) *Total proportionality* (II); (iii) Incremental proportionality (III), and (iv) Continuity in ρ (IV).

Physically the property (II) means that a protocol starting from an uncorrelated initial state and using l qubits or $2l$ classical bits of communication and local operations should not create more than $2l$ bits of correlation. The property (III) means that one may expect that the transmission of l qubits or $2l$ classical bits should not increase the correlation of any initial state by more than $2l$ bits. All of these properties (I-IV) hold for some known correlation measures. They hold for the classical mutual information $I(A:B)$ when communication is classical as one may expect. For example, (total and) incremental proportionality of $I(A:B)$ for the classical case follows from the fact that: $\max\left(H(p_A),H(p_B)\right)\le H(p_{AB})\le H(p_A)+H(p_B)$, so that when A sends a classical system A' to B, $I_{Cl}(\rho)=I(A;BA')\le I(AA';B)+H(p_{A'})$. Total proportionality then follows from incremental proportionality. They also hold for the quantum mutual information

$$I_Q(A:B)=S(\rho_A)+S(\rho_B)-S(\rho_{AB}).$$

The surprising fact that incremental proportionality for $I_{Cl}(\rho)$ can be violated in some extreme manner for a mixed initial state ρ: A single classical bit, sent from A to B, can result in an arbitrary large increase in $I_{Cl}(\rho)$ [8, 50].

This phenomenon can be viewed as a way of locking classical correlation in the quantum state ρ.

Since incremental proportionality of $I_{Cl}(\rho)$ holds classically, the phenomenon of locked correlation is purely quantum effect. It is direct consequence of the indistinguishability of non-orthogonal quantum states.

Example. For a given initial state ρ and the amount and type of communication, it is possible quantify the increase in correlation by defining the following functions [50]:

$$\text{(i) } I_{Cl}^{(l)}=\max_{\Lambda^{(l)}} I_{Cl}\left(\Lambda^{(l)}(\rho)\right) \text{ (one-way classical communication)};$$

$$\text{(ii) } I_{Cl}^{[l]}=\max_{\Lambda^{[l]}} I_{Cl}\left(\Lambda^{[l]}(\rho)\right) \text{ (two-way classical communication)}.$$

The operator Λ denotes a bipartite quantum operation that consists of local operations and no more than l bits or qubits of communication, a constraint denoted by the superscript (l) or $[l]$, respectively. We use ρ and ρ' to denote the states before and after the quantum operation with communication, $\rho'=\Lambda(\rho)$.

The amount of correlation unlocked by l bits of one-way classical communication $I_{Cl}^{(l)}(\rho)$ can be bounded as [8, 38]: $I_{Cl}^{(l)}(\rho)-I_{Cl}(\rho)\le l+\left(2^l-1\right)I_{Cl}(\rho)$. For small $I_{Cl}(\rho)$, the amount unlocked by l qubits (two-way) can be bounded:

$$I_{Cl}^{[l]}(\rho)-I_{Cl}(\rho)\le 2l+O\left(d^2\sqrt{I_{Cl}(\rho)}\log I_{Cl}(\rho)\right).$$

A3.2. *Hidden (locking) classical correlation in quantum state*. Let us now discuss the situation in which an arbitrary amount of correlation is unlocked with a one-way message. The initial state ρ is shared between subsystems held by A and B, with respective dimensions $2d$ and d,

$$\rho = \frac{1}{2d}\sum_{k=0}^{d-1}\sum_{t=0}^{1}\left(|k\rangle\langle k|\otimes|t\rangle\langle t|\right)_A \otimes \left(U_t|k\rangle\langle k|U_t^\dagger\right)_B .$$

Here $U_0 = I$ and U_1 changes the computational basis to a conjugate basis: $\left|\langle i|U_1|k\rangle\right| = \frac{1}{\sqrt{d}} \quad \forall\, i,k$.

In this case, B's is given a random draw $|k\rangle$ from d states in two possible random bases (depending on whether $t=0$ or 1), while A has complete knowledge on his state. To achieve $I_{Cl}^{(l)}(\rho) = \log d + 1$, A sends t to B, who then undoes U_t on his state and measure k in the computational basis. A and B now share both k and t, with $I_{Cl}^{(l)}(\rho) = \log d + 1$ bits of correlation.

The state ρ can arise from following scenario. Let $d = 2^n$. A picks a random n-bit string k and sends B $|k\rangle$ or $H^{\otimes n}|k\rangle$ depending on whether the random bit $t=0$ or 1. Here H is the Hadamard transform. A can send t to B to unlock the correlation later. Experimentally, Hadamard transform and measurement on single qubits are sufficient to prepare the state ρ and later extract the unlocked correlation in ρ'.

The initial correlation is small, $I_{Cl}^{(l)}(\rho) = \frac{1}{2}\log d$. The final amount of information after the complete measurement M_A in one-way communication is as $I_{Cl}(\rho') = I_{Cl}^{(l)}(\rho) = \log d + 1$, i.e., the amount of accessible information increase.

First, the complete measurement M_A in the basis $\{|k\rangle\otimes|t\rangle\}$ is provable optimal for A: Since the outcome tells her precisely which pure state from the ensemble she has, she can apply *classical*, *local* post-processing to obtain the output distribution for any other measurement she could have performed. For A's choice of optimal measurement, $I_{Cl}(\rho)$ is simply B's *accessible* information I_{Acc} about the uniform ensemble of states

$$\left\{|k\rangle, (U_1 = H)|k\rangle\right\}_{k=0,\dots,d-1} .$$

A3.3. *Accessible information about ensemble of mixed states.* In general, the accessible information about ensemble of mixed states $\mathcal{E} = \{p_i, \eta_i\}$ is the maximal mutual information between i and the outcome of a measurement. $I_{Acc}(\mathcal{E})$ can be maximized by a POVM with rank 1 elements only [5, 8]. Let $M = \left\{\alpha_j |\phi_j\rangle\langle\phi_j|\right\}_j$ stand for a POVM with rank 1 elements where each $|\phi_j\rangle$ is normalized and $\alpha_j > 0$. Then $I_{Acc}(\mathcal{E})$ can be expressed as following:

$$I_{Acc}(\mathcal{E}) = \max_M \left[\underbrace{-\sum_i p_i \log p_i}_{\text{Classical Part}} + \underbrace{\sum_i \sum_i p_i \alpha_j \langle\phi_j|\eta_i|\phi_j\rangle \log \frac{p_i\langle\phi_j|\eta_i|\phi_j\rangle}{\langle\phi_j|\mu|\phi_j\rangle}}_{\text{Quantum Part}} \right],$$

where $\mu = \sum_i p_i \eta_i$. We now apply this equation to the abovementioned problem. The ensemble is $\left\{\frac{1}{2d}, U_t|k\rangle\right\}_{k,t}$ with $i = k,t$; $p_{k,t} = \frac{1}{2d}$, $\mu = \frac{I}{2}$ and $\langle\phi_j|\mu|\phi_j\rangle = \frac{1}{d}$.

Putting all these in abovementioned equation for $I_{Acc}(\mathcal{E})$ we have the following:

$$I_{Cl}(\mathcal{E}) = \max_M \left[\underbrace{\log 2d}_{\text{Classical Part}} + \underbrace{\sum_{j,k,t} \frac{\varepsilon_j}{2d} \left|\langle \phi_j | U_t | k \rangle\right|^2 \log \frac{\left|\langle \phi_j | U_t | k \rangle\right|^2}{2}}_{\text{Quantum Part}} \right]$$

$$= \max_M \left[\underbrace{\log d}_{\text{Classical Part}} + \underbrace{\sum_j \frac{\alpha_j}{d} \left(\frac{1}{2} \sum_{k,t} \left|\langle \phi_j | U_t | k \rangle\right|^2 \log \left|\langle \phi_j | U_t | k \rangle\right|^2 \right)}_{\text{Quantum Part}} \right]$$

where we use $\sum_j \alpha_j = d$ and $\forall j,t \;\; \sum_k \left|\langle \phi_j | U_t | k \rangle\right|^2 = 1$ to obtain the last term. Since $\sum_j \frac{\alpha_j}{d} = 1$, the second term is a convex combination, and can be upper bounded by maximization over just one term:

$$I_{Cl}(\mathcal{E}) \le \log d + \max_{|\phi\rangle} \frac{1}{2} \sum_{k,t} \left|\langle \phi | U_t | k \rangle\right|^2 \log \left|\langle \phi | U_t | k \rangle\right|^2 .$$

Remark. Note that $-\sum_{k,t} \left|\langle \phi | U_t | k \rangle\right|^2 \log \left|\langle \phi | U_t | k \rangle\right|^2$ is the sum of the entropies of measuring $|\phi\rangle$ in the computation basis and the conjugate basis. Such a sum of entropies is at least $\log d$. Lower bounds of these type are called *entropic uncertainty inequalities* (EUI), which quantity how much a vector $|\phi\rangle$ cannot be simultaneously aligned with states from two conjugated bases. It follows that: $I_{Cl}(\rho) \le \frac{1}{2} \log d$.

Equality can in fact be attained when B measures in the computational basis, so: $I_{Cl}(\rho) = \frac{1}{2} \log d$, and,

$$I_{Cl}^{(l)}(\rho) - I_{Cl}(\rho) = 1 + \frac{1}{2} \log d .$$

We also remark that the incremental proportionality remains violated for multiple copies of ρ. Wootters proved [8] that the accessible information from m independent draws of an ensemble $\mathcal{E}$ of separable states is additive, $I_{Acc}\left(\mathcal{E}^{\otimes m}\right) = m I_{Acc}(\mathcal{E})$. It follows $I_{Cl}\left(\rho^{\otimes m}\right) = m I_{Cl}(\rho)$ in this case.

Example. Given the bipartite state ρ_{AB} a possible measure of the *classical correlation* between subsystems A and B is

$$Cor_B(\rho_{AB}) = \max_B \left[S(\rho_A) - \sum_i p_i S\left(\rho_A^i\right) \right] \quad \text{(A3.2)}$$

where $\rho_A = Tr_B(\rho_{AB})$ is reduced density matrix. The von Neumann entropy is $S(\rho) = -Tr(\rho \log \rho)$. The conditional density matrix ρ_A^i is the density matrix of A after performing the measurement B_i over B: $\rho_A^i = \frac{Tr_B(B_i \rho_{AB})}{Tr_{AB}(B_i \rho_{AB})}$. The probability of A being in the state ρ_A^i is $p_i = Tr_{AB}(B_i \rho_{AB})$.

The correlation measure (1) has a simple physical interpretation: if A and B are not correlated then the marginal entropy of A $\left[S(\rho_A)\right]$ and the residual entropy of A after a POVM measurement on B $\left[\sum_i p_i S\left(\rho_A^i\right)\right]$ should coincide to give $Cor_B(\rho_{AB}) = 0$, since for an uncorrelated system AB, A is not affected by a POVM measurement on B. Moreover, note that $\rho_A = \sum_i p_i \rho_A^i$; hence for a given POVM B the combination as $\left[S(\rho_A) - \sum_i p_i S(\rho_A^i) \right]$ is closely related to the entropy defect defined by L. Levitin (1969).

So the classical correlation $Cor_B(\rho_{AB})$ can be seen as the maximum average decrease in the entropy of the system A when a state ρ_A^i (after a measurement B_i is performed on B) is specified compared with a situation when only the mixture of states ρ_A is known. The classical correlation is a measure of how strong the two subsystems are correlated no matter which subsystem is used to extract such a correlation.

Remark. The quantum mutual information $I(A:B)$ of a bipartite system AB can be decomposed into an information deficit (or work deficit) Δ and the classical information deficit Δ_{cl}: $I = \Delta_{cl} + \Delta$. So naturally one should be concerned with an analogous decomposition of the mutual information when using different measures of classical correlation. Also the estimated classical correlation and the relative entropy of entanglement (E_{REn}) do not add up to give the von Neumann mutual information between the two subsystems, i.e., $I(\rho_{A:B}) > [C_B(\rho_{AB})]_{opt} + E_{REn}$. It is means that a more elaborate choice of POVM may saturate the total correlations.

By considering all possible POVM's for a given state, the optimal POVM cannot saturate the total correlations. Another alternative, which renders the definitions of classical correlations compatible with the mutual information, is the possibility of having a different definition of quantum correlations, which is different from (E_{REn}). A possible candidate is the quantum discord. It is result of the difference between classical and quantum conditional entropies. In contrast to classical conditional entropy, quantum conditional entropy is a measurement dependent quantity.

<u>*Example*</u>: *Mutual information and quantum discord*. In contrast to classical conditional entropy, quantum conditional entropy is a measurement dependent quantity. The quantum discord is defined as

$$\delta(A:B) = I(A:B) - J(A:B)_{\{\Pi_i^B\}}.$$

J is the information gained about B as a result of the set of measurements $\{\Pi_i^B\}$:

$$J(A:B)_{\{\Pi_i^B\}} = S(A) - S\left(A \middle| \{\Pi_i^B\}\right) = S(A) - \sum {}^{*}p_i S\left({}^{*}\rho_i^A\right),$$

where ${}^{*}p_i$ and ${}^{*}\rho_i^A$ were defined originally as the special case of p_i and ρ_i^A when the choice of the set of measurement is restricted to one-dimensional projectors Π_i^B. The above definition of the quantum discord reflects clearly the inherent measurement dependence of the quantum conditional entropy. For the quantum discord to be zero one has to find at least one measurement for which it is zero. Therefore the minimum of the quantum discord is relevant quantum correlation. By focusing on perfect measurements of B, defined by a set of one-dimensional projectors, one can easily check that the set of measurements that minimizes the quantum discord, i.e., maximizes J, is exactly the same POVM set that optimizes the classical correlations for binary states. This follows from the definition of both quantities, and the result on the optimization of classical correlation using projective measurement only. Hence, $\max\left[J(A:B)_{\{\Pi_i^B\}} \right] = Cor_B(\rho_{AB})$. Therefore,

$$I(A:B) = Cor_B + \min_{\{\Pi_i^B\}} \delta(A:B),$$

i.e., for binary states the classical correlation and the quantum discord add up to give the mutual information.