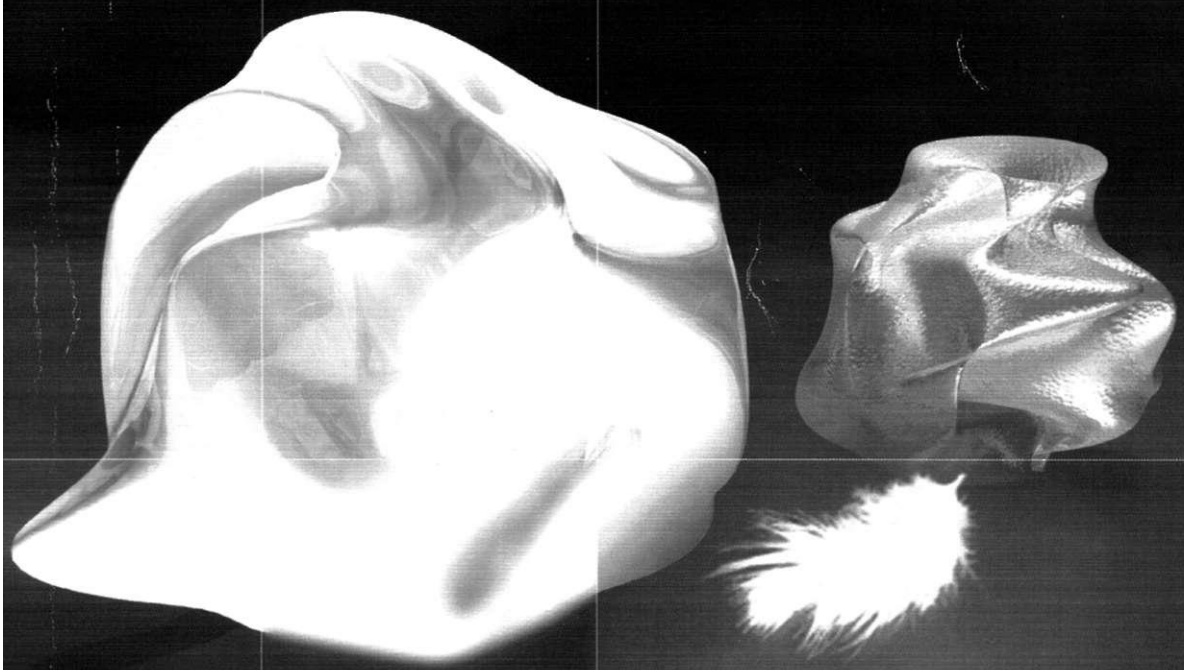
Том 3, № 3, Сентябрь 2008 ISSN 1819-4362

НЕЧЕТКИЕ СИСТЕМЫ и мягкие вычисления



Научный журнал Российской ассоциации
нечетких систем и мягких вычислений

УДК 658.012.011.56

CLASSICAL EFFICIENT SIMULATION OF WISE QUANTUM CONTROL IN NON-LINEAR DYNAMIC SYSTEMS BASED ON QUANTUM GAME GATES

Ulyanov S.V., Degli Antoni G., Nesterenko M.S., Yamafuji K.
International University of Nature, Society, and Man "Dubna", Moscow, Russia
Universita di Milano, Crema, Italy
University of Electro-Communications, Chofu, Tokyo, Japan

Поступила в редакцию 15.03.2008.

Предлагается обобщение игры Парродо (с запутанными состояниями) и квантовой игры без запутанных состояний для применения в системах интеллектуального управления. Рассматривается применение нечётких квантовых вычислений как основы для технологии создания систем интеллектуального управления. Предлагается подход к аппаратной реализации квантовых вычислений для моделирования и создания систем управления для приложений интеллектуальной мехатроники. Описывается архитектура системы интеллектуального нечёткого управления, основанная на данном подходе.

New effect in design of intelligent control systems as a generalization of *Parrondo* (entangled) game and card quantum entanglement-free game (without entanglement) is considered. Applied Quantum Soft Computing (as a tool and background for design technology of robust intelligent control) is considered. Quantum algorithm game gate (QAGG)-approach for HW-implementation of fast quantum algorithms in simulation and design of AI-robotics and smart mechatronics control systems is developed. Intelligent control system design with wise robust fuzzy controller based on QAGG-approach is also described.

Ключевые слова: квантовые вычисления, искусственный интеллект, квантовые игры, интеллектуальное робастное управление.
Keywords: Quantum gate computing, AI-system, Quantum games, Wise robust control.

1. Introduction

We consider the application of the quantum algorithm gate (QAG)-design approach to the classical efficient simulation of quantum games. In [1] we discussed some important applications (as example, quantum games and decision-making control processes in quantum uncertainty of information) of Quantum Soft Computing tool in AI-systems. Using Benchmark's method, different quantum paradigms and methods of AI (on examples from quantum games) are demonstrated in present article. Their applications in problem solution of theoretical informatics (TI) and computer science (Grover's QAG) to design intelligent robust control systems of essentially non-linear

dynamic control objects (as background of intelligent robotics and mechatronics) based on Quantum Soft Computing models are described. We study a new problem in applied intelligent control system: design of wise robust control laws using non-robust particular knowledge bases (KBs) that are designed with soft computing technology. This problem is correlated with the solutions of well-known Parrondo quantum game and quantum card game without entanglement. As result, the possibility to design a wise robust control from non-robust KBs using quantum computing without entanglement is found. This approach is different from the methods of quantum games [1] where the entanglement plays key role.

2. Quantum soft computing as a new paradigm in simulation of AI-control systems: Quantum game gates approach

Classical Artificial Intelligence (AI) and Theoretical Informatics (TI) are based on the assumption that information processing (taking place in the circuits of a human brain) can be simulated by classical computation. The basis of classical computation is the *Church-Turing* thesis, which says that every recursive function can be computed algorithmically, provided algorithm can executed by a physical process. Classical computation is based on classical (Boolean) logic and can be viewed as an embodiment of classical physics. For example, AI (based on classical model of computation) consists of two parts: (*i*) symbolic approach to AI (based on classical Boolean logic) and its application; (*ii*) soft computing approach to AI based on non-classical logic (for example, on fuzzy/ probabilistic logic etc.) and its applications.

However, fundamental physical processes are not governed by classical mechanics, rather by quantum mechanical laws. If, as an example the brain performs quantum processing, this might be the secret behind consciousness. Recent investigations in the area of quantum information processing and communications (as a main basic scientific goals of TI and computer science) made clear that the foundations of computing have to be based not on the laws and limitations of the classical physics as so far, but on the laws and limitations of quantum physics. The possibility of performing reversible computation and the fact that classical computers cannot efficiently simulate quantum systems gave birth to the concept of the quantum Turing machine as the generalization of the *Church-Turing* thesis. This led to a flurry of discoveries in quantum computation and information, quantum algorithms (QA's), quantum simulators, quantum automaton and programmable gate array [2 - 7]. Furthermore, it might explain several puzzling features of animal and human intelligence and provide a new direction to develop AI-systems based on quantum computation [8]. Quantum computation can be viewed as an embodiment of quantum physics and is founded on *superposition* of quantum mechanics logic and new non-classical phenomena as *quantum entanglement* (quantum correlation) and *quantum interference*, which are entirely different paradigms in global optimization and consciousness learning processes. In general, quantum computing can be considered as a quantum control of computational process in open information-thermodynamic system [9]. Background of Quantum Soft Computing is quantum algorithm gate (QAG) design method and classical efficient simulation system of QAG's [10 - 13]. We are discussed in [10, 12] a new method of simulation and physical silicon implementation of QAG's with applications to robust intelligent control. R&D results in simulation and design of QAG are described. The developed analysis and synthesis of QAG's dynamic is the background for silicon circuit gate design and simulation of robust knowledge base

(KB) for intelligent fuzzy controllers. The QAG's design method on the example as Grover's quantum search algorithm is illustrated. In present article, using Benchmark's method, different quantum paradigms and methods of AI (on examples from quantum games), and their applications in problem solution of TI and computer science (Grover's quantum search algorithm gate design and simulation), and design of intelligent robust control systems of essentially non-linear dynamic control objects based on Quantum Soft Computing model [8, 12, 14] are described.

Game (see Table 1 in [1]): *Parrondo's Paradox.* The Parrondo's game is one in which a random combination of two losing games produces a winning game [15, 16]: two separate losing games can be combined following a random or period strategy in order to have a resulting winning game.

Classical version of Parrondo Paradox (Brownian ratchet). Two statistically losing games of chance as game **A** and game **B** are combined following a random or periodic strategy in order to have a resulting winning game. In the original version of Parrondo's paradox [15] it is demonstrated by tossing coins where the coins are biased towards winning or losing. In particular: (1) game **A** consists of a biased coin 0, which has the probability p of winning; (2) game **B** can be described by the following statement. If the present capital is a multiple of Mthen the chance of winning isp_1, if it is not a multiple of M the chance of winning isp_2. It has been proved [15] that the game **A** results a loosing game when the following condition is met: $\frac{1-p}{p} > 1$ while game **B** is loosing when$\frac{(1-p_1)(1-p_2)^{M-1}}{p_1 p_2^{M-1}} > 1$. A resulting game $A \oplus B$ can be constructed by random switching between games **A** and **B** with probabilityγ. This game is capital-dependent game. It was established [15] that there are choices of p, p_1 and p_2 such that games **A** and **B** are both losing, but the resulting game is winning.

This behavior has been termed *Parrondo's Paradox.* By regarding the current capital as the state of a discrete-time Markov chain, it has been shown in [15] that the paradox exists if the following condition is met:

$$\frac{(1-q_1)(1-q_2)^{M-1}}{q_1 q_2^{M-1}} > 1; \quad q_1 = \gamma p + (1-\gamma) p_1; \quad q_2 = \gamma p + (1-\gamma) p_2.$$

In quantum Parrondo's Paradox, rotation operators (that represent the toss of classical biased coin) are replaced by general operators from $SU(2)$ to transform the game into the quantum domain. Comparing to previous realization of classical Parrondo's games(A, B), the rotating-vector realization produces a much higher winning rate for the combined game $(A \oplus B)$even though the losing rates for games $(A, B)$are greater [16]. In classical gambling games there is a random element, and in a Parrondo's game, the results of the random process are used to alter the evolution of game. The quantum mechanical model is deterministic until a measurement is made at the end of the process. The element of chance, which is necessary in the classical game, is replaced by a superposition that represents all the possible results in parallel. We can get new behavior by the addition of phase factors in the operators and by *interference* between states. The information flow for the case of two games of (A) followed by one game of (B) is shown in Figure 1a.

The gameA: The quantum analogue of a single toss of a biased coin. An arbitrary $SU(2)$ operation can be written as

$$\hat{A} = \hat{P}(\gamma)\,\hat{R}(\theta)\,\hat{R}(\delta) = \begin{pmatrix} e^{-i\frac{1}{2}(\gamma+\delta)}\cos\theta & -e^{-i\frac{1}{2}(\gamma-\delta)}\sin\theta \\ e^{-i\frac{1}{2}(\gamma-\delta)}\sin\theta & e^{i\frac{1}{2}(\gamma+\delta)}\cos\theta \end{pmatrix} \qquad (1)$$

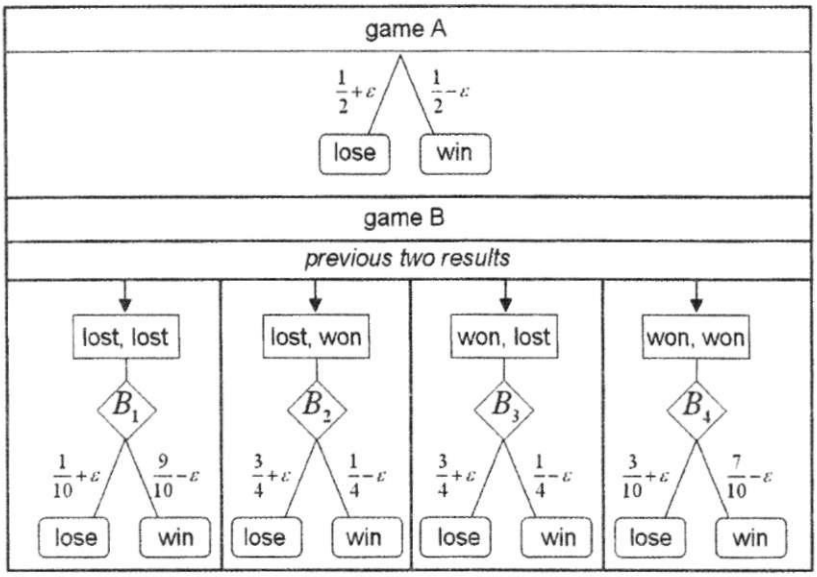


Figure 1a: Winning and loosing probabilities for game A and the history dependent game B

where $\theta \in [-\pi, \pi]$and $\gamma, \delta \in [0, 2\pi]$.

Game B. Four SU (2) operations, each of the form of Eq. (1), whose use is controlled by the results of the previous two games used in this game:

$$\hat{B}(\phi_i, \alpha_i, \beta_i) = diag[A_i(\phi_i, \alpha_i, \beta_i)], \ i = 1, 2, 3, 4.$$

Quantum algorithm and Parrondo's QAG. Operator $\hat{B}$ acts on the state$|\psi - 2\rangle \otimes |\psi - 1\rangle \otimes |i\rangle$, where $|\psi - 1\rangle$ and $|\psi - 2\rangle$ represent the result of the two previous games and $|i\rangle$ is the initial state of the target qubit. That is$\hat{B}|q_1 q_2 q_3\rangle = |q_1 q_2 b\rangle$, where $q_1, q_2, q_3 \in \{0, 1\}$and b is output of game$B$. The sequence (AAB)played n times results in the state as in Table 1 from [1].The expectation value of the payoff from a sequence of games resulting in the state $|\psi_{fin}\rangle$ can be computed by

$$\langle \$ \rangle = \sum_{j=0}^{n} \left((2j - n) \sum_{j'} \left| \left\langle \psi_j^{j'} \mid \psi_{fin} \right\rangle \right|^2 \right), \tag{2}$$

where the second summation is taken over all basis states $\left\langle \psi_j^{j'} \right|$ with j 1's and $(n-j)$ 0's. If the initial state is a superposition, then payoffs different from the classical game can be obtained as a result of interference. We may obtain much larger or smaller payoffs provided the initial state involves a superposition that gives the possibility of interference for that particular game sequences.

Consider the game sequence $(AAB)$from Figure 1b.

In order to get interference there needs to be two different ways of arriving at the same state. We need only to choose some superposition not the maximally entangled state; however, this is the most interesting initial state to study. Choosing GHZ-state

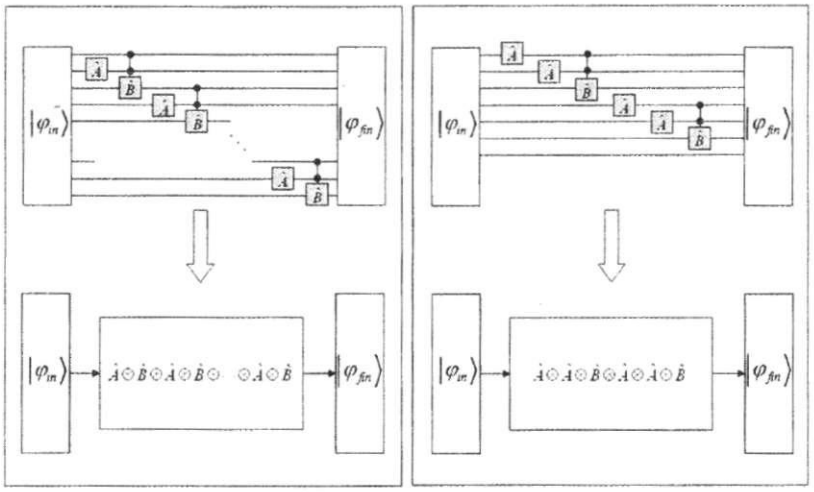


Figure 1b: The information flow in qubits

as $|\psi_i^m\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ the result

$$\langle \$_{AAB}^m \rangle = \tfrac{1}{2}\cos 2\theta\,(\cos 2\phi_4 - \cos 2\phi_1) + \tfrac{1}{4}\sin^2 2\theta \begin{pmatrix} \cos(2\delta+\beta_1)\sin 2\phi_1 \\ -\cos(2\delta+\beta_1)\sin 2\phi_2 - \cos(2\delta+\beta_3)\sin 2\phi_3 + \cos(2\delta+\beta_4)\sin 2\phi_4 \end{pmatrix}. \quad (3)$$

In Eq. (3) the value of $\langle \$_{AAB}^m \rangle$depends on the phase angles δ and β_i that can produce a result that cannot be obtained in the classical game. The entanglement and the resulting interference can make game B in the sequence (AAB) better than its best branch taken alone. Indeed the expectation for payoff of a quantum (AAB_1) on the maximally entangled initial state vanishes due to destructive interference. An initial state that is a different superposition may give *interference* effects [16].

Remark. In the quantum games, we can see that in the decision-making step the player has means of communication with each other, i.e., no one has any information about which strategy the other player will adopt. This is the same as in classical game. A fascinating property in quantum game is entanglement. Although there is no communication between the two players, the two qubits are entangled, and therefore one player's local action on his qubit will affect the state of the other. Entanglement plays as a contract of the game [16 - 24]. Let us consider involving quantum algorithms, in which cooperating with randomness may be a better strategy than trying to fight it.

Example: *Grover's QSA as quantum game* [19]. We consider a game where the player's goal is to obtain (i.e., measure with a high probability) a fixed, unknown number α, $0 \leqslant \alpha \leqslant 2^n - 1$ in as few time steps as possible. The initial state has the form$|\psi_{in}\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle$. In this game, an infinite sequence of operators (quantum oracles) $\hat{O}_1 \ldots \hat{O}_m$will be applied to$|\psi_{in}\rangle$. The player decides when he would stop the sequence, i.e., he has the freedom to choose m such that$|\psi_{fin}\rangle = \hat{O}_m \ldots \hat{O}_1 |\psi_{in}\rangle$. The

payoff is then determined in the computational basis of$|\psi_{fin}\rangle$. The game is winning if the player possesses a strategy that wins with probability $> \frac{1}{2}$, and is losing otherwise.

This game incorporates strategic moves, since the set used by the player to decide the duration of the game are equivalent to the set of natural numbers **N**.

Game A. Here $\hat{O}_i = \hat{A}$ for all$i$, where$\hat{A}(|x\rangle) = (-1)^{\delta_{x\alpha}}|x\rangle$. Geometrically, $\hat{A}$ reflects the vector $|\psi_{in}\rangle$ about$|\alpha\rangle$. Since$\hat{A}^2 = I$, the player's freedom in choosing when to stop the game always reduces to just one of the following two scenarios: $|\psi_{fin}\rangle = \hat{A}|\psi_{in}\rangle$ or$|\psi_{fin}\rangle = |\psi_{in}\rangle$. Unfortunately for the player, the payoff is $\left|\langle\alpha|\hat{A}|\psi_{in}\rangle\right|^2 = |\langle\alpha \mid \psi_{in}\rangle|^2 = \frac{1}{2^n}$ which less than is $\frac{1}{2}$ for$n \geqslant 2$.

Therefore, for player does not possess a winning strategy, hence game **A** is losing for him.

Game B. Here $\hat{O}_i = \hat{B}$ for all$i$, where$\hat{B} = 2|\psi_{in}\rangle\langle\psi_{in}| - I$. Geometrically, $\hat{B}$ reflects $|\psi_{in}\rangle$ about itself. Again, the player has the freedom to decide how many $\hat{B}$ are applied to the input state before measurement. However, since$|\psi_{in}\rangle = \hat{B}|\psi_{in}\rangle$, the player can have no influence in determining the payoff in this game. The game is hence losing for him because the payoff $|\langle\alpha \mid \psi_{in}\rangle|^2 = \frac{1}{2^n}$ which is less than$\frac{1}{2}$.

Game$A \oplus B$. The player combines games **A** and **B** at random. By this, it means $\hat{O}_i = \hat{A}$ or $\hat{B}$ with equal probability. Once again, the player has the freedom to decide when to stop the sequence and hence do the measurement. Since $\hat{A}^2 = \hat{B}^2 = Iand|\psi_{in}\rangle = \hat{B}|\psi_{in}\rangle$, any given finite sequence $\hat{O}_i$ will always produce a final state with the following form:

$$|\psi_{fin}\rangle = \left(\hat{B}\right)\hat{A}\hat{B}\ldots\hat{A}\hat{B}\hat{A}|\psi_{in}\rangle.$$

Now, numerical calculation suggests that for$m = 4k$,

$$|\psi_{fin}\rangle = \hat{O}_m\ldots\hat{O}_1|\psi_{in}\rangle = \underbrace{\left(\hat{B}\hat{A}\right)\ldots\left(\hat{B}\hat{A}\right)}_{k\ times}|\psi_{in}\rangle.$$

It can also be seen that $\hat{B}\circ\hat{A} = \hat{G}$ is Grover's operator (see Appendix in details). Hence a winning strategy for the player is to stop after $(4k)$-th operation where$K = \left\lceil\frac{\pi}{4}\sqrt{2^n}\right\rceil$.

The winning probability is $> \frac{1}{2}$, and hence we see that this combined game is winning for the player [19].

We are interested in the classical-quantum game where one player, say **A**, is restricted to S_{Cl}while the other, **B**, has access to quantum strategyS_{Qt}.

Example: Classical-quantum game [23]. As mentioned in [1] (Eq. (2.6)), a pure quantum strategy $\hat{U}(\theta,\alpha,\beta)$ is an $SU(2)$ operator and may be written as

$$\hat{U}(\theta,\alpha,\beta) = \begin{pmatrix} e^{i\alpha}\cos\frac{\theta}{2} & ie^{i\beta}\sin\frac{\theta}{2} \\ ie^{-i\beta}\sin\frac{\theta}{2} & e^{-i\alpha}\cos\frac{\theta}{2} \end{pmatrix},$$

where $\theta \in [0,\pi]$ and $\alpha,\beta \in [-\pi,\pi]$. Let us consider the particular cases of this operation.

1) *A classical mixed strategy.* It can be simulated in the quantum game protocol by an operator in the set$S_{Cl} \equiv \hat{U}(\theta) = \hat{U}(\theta,0,0)$. Such a strategy corresponds to playing $\hat{I}$ with probability $\cos^2\frac{\theta}{2}$ and $\hat{F}$ with probability$\sin^2\frac{\theta}{2}$. Where both players use such strategies the game is equivalent to the classical game.

2) *Quantum game strategies.* When both players have access to the full set of quantum operators, for any$\hat{A} = \hat{U}(\theta,\alpha,\beta)$, there exists$\hat{B} = \hat{U}\left(\theta,\alpha,-\frac{\pi}{2}-\beta\right)$, such

that

$$\left(\hat{A}\otimes\hat{I}\right)\frac{1}{\sqrt{2}}\left(|00\rangle+|11\rangle\right)=\left(\hat{I}\otimes\hat{B}\right)\frac{1}{\sqrt{2}}\left(|00\rangle+|11\rangle\right).$$

That is, on the maximally entangled state, any local unitary operation that **A** carries out on her qubit is equivalent to a local unitary operation that **B** carries out on his.

Hence either player can undo his/her opponent's move (assuming it is known) by choosing $\hat{U}\left(\theta,-\alpha,\frac{\pi}{2}-\beta\right)$ in response to$\hat{U}\left(\theta,\alpha,\beta\right)$. Indeed, knowing the opponent's move, each player can produce any desired final state.

3) *Classical-quantum game strategies.* In the classical-quantum game where one player, say **A**, is restricted to $S_{Cl}\equiv\left\{\hat{U}\left(\theta\right):\theta\in[0,\pi]\right\}$while the other, **B**, has access to

$$S_{Qt}=\left\{\hat{U}\left(\theta,\alpha,\beta\right):\theta\in[0,\pi],\alpha,\beta\in[-\pi,\pi]\right\}.$$

In this case $\hat{U}\left(\theta\right)$doesn't necessary the same results as a classical mixed strategy since **B** can exploit the *entanglement* to his advantage. Nevertheless we shall refer to strategies in S_{Cl} as "classical"in the sense that the player does not manipulate the phase of the qubit. In this situation **B** has a distinct advantage since only he can produce any desired final state by local operations on his qubit. Without knowing **A**'s move, **B**'s best plan is to play the "miracle" quantum move, consisting of assuming that **A** has played with quantum strategy $\hat{U}\left(\frac{\pi}{2}\right)$, the average move from S_{Cl}, undoing this move by $\hat{V}=\hat{U}\left(\frac{\pi}{2},0,\frac{\pi}{2}\right)=\frac{1}{\sqrt{2}}\begin{pmatrix}1&-1\\1&1\end{pmatrix}$and that preparing his desired final state. The operator $\hat{f}=\begin{pmatrix}0&1\\-1&0\end{pmatrix}$ has the property$\left(\hat{I}\otimes\hat{f}\right)\frac{1}{\sqrt{2}}\left(|00\rangle+i\,|11\rangle\right)=\left(\hat{F}\otimes\hat{I}\right)\frac{1}{\sqrt{2}}\left(|00\rangle+i\,|11\rangle\right)$, so **B** can effectively flip **A**'s qubit as well as adjusting his own.

Example: Suppose we have a general 2×2 game with payoffs [20 - 24]

Player	**B: 0**	**B: 1**
A: 0	(p,p')	(q,q')
A: 1	(r,r')	(s,s')

where unprimed values refer to **A**'s payoffs and the primed to **B**'s. **B** has four possible miracle moves depending on the final state that prefers:

$$\hat{M}_{00}=\hat{V}=\frac{1}{\sqrt{2}}\begin{pmatrix}1&-1\\1&1\end{pmatrix}\quad\hat{M}_{01}=\hat{F}\hat{V}=\frac{i}{\sqrt{2}}\begin{pmatrix}1&-1\\1&1\end{pmatrix}$$
$$\hat{M}_{10}=\hat{f}\,\hat{V}=\frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\-1&1\end{pmatrix}\quad\hat{M}_{11}=\hat{F}\,\hat{f}\,\hat{V}=\frac{i}{\sqrt{2}}\begin{pmatrix}-1&1\\1&1\end{pmatrix}$$

given a preference for $|00\rangle,|01\rangle,|10\rangle$ and $|11\rangle$, respectively. In the absence of entanglement, any $\hat{M}_{ij}$ is equivalent to $\hat{U}\left(\frac{\pi}{2}\right)$ that is, the mixed classical strategy of flipping or not-flipping with equal probability. When we use an entangling operator $\hat{J}\left(\gamma\right)$ for an arbitrary$\gamma\in\left[0,\frac{\pi}{2}\right]$, the expectation value of **A**'s payoff if she play $\hat{U}\left(\theta\right)$ against **B**'s miracle move are, respectively,

$$\begin{aligned}
\langle\$_{00}\rangle &= \tfrac{p}{2}\left(\cos\tfrac{\theta}{2}+\sin\tfrac{\theta}{2}\sin\gamma\right)^2+\tfrac{q}{2}\cos^2\left(\tfrac{\theta}{2}\right)\cos^2\gamma+\tfrac{r}{2}\left(\sin\tfrac{\theta}{2}-\cos\tfrac{\theta}{2}\sin\gamma\right)^2+\tfrac{s}{2}\sin^2\left(\tfrac{\theta}{2}\right)\cos^2\gamma\\
\langle\$_{01}\rangle &= \tfrac{p}{2}\cos^2\left(\tfrac{\theta}{2}\right)\cos^2\gamma+\tfrac{q}{2}\left(\cos\tfrac{\theta}{2}+\sin\tfrac{\theta}{2}\sin\gamma\right)^2+\tfrac{r}{2}\sin^2\left(\tfrac{\theta}{2}\right)\cos^2\gamma+\tfrac{s}{2}\left(\sin\tfrac{\theta}{2}-\cos\tfrac{\theta}{2}\sin\gamma\right)^2\\
\langle\$_{10}\rangle &= \tfrac{p}{2}\left(\cos\tfrac{\theta}{2}-\sin\tfrac{\theta}{2}\sin\gamma\right)^2+\tfrac{q}{2}\cos^2\left(\tfrac{\theta}{2}\right)\cos^2\gamma+\tfrac{r}{2}\left(\sin\tfrac{\theta}{2}+\cos\tfrac{\theta}{2}\sin\gamma\right)^2+\tfrac{s}{2}\sin^2\left(\tfrac{\theta}{2}\right)\cos^2\gamma\\
\langle\$_{11}\rangle &= \tfrac{p}{2}\cos^2\left(\tfrac{\theta}{2}\right)\cos^2\gamma+\tfrac{q}{2}\left(\cos\tfrac{\theta}{2}-\sin\tfrac{\theta}{2}\sin\gamma\right)^2+\tfrac{r}{2}\sin^2\left(\tfrac{\theta}{2}\right)\cos^2\gamma+\tfrac{s}{2}\left(\sin\tfrac{\theta}{2}+\cos\tfrac{\theta}{2}\sin\gamma\right)^2
\end{aligned}$$

where primes to p, q, r and s to get **B**'s payoffs are added. Although the miracle moves are in some sense best for **B**, in that they guarantee a certain minimum payoff against any classical strategy from **A**, there is not necessarily any NE amongst pure strategies in the classical-quantum game.

Role of entanglement parameterγ. In each of the four cases in above mentioned table there are critical values of the entanglement parameter γ below which the quantum player no longer has an advantage. The most interesting games are those that contain some sort of dilemma for the players. The games, along with some important equilibrium, are summarized [1] in Table 1.

A summary of the thresholds for the collection of games is given according to [1] in Table 2.

In the following, the payoffs shall be designated a, b, c and d with$a > b > c > d$. The two pure classical strategies for the players are referred to as cooperation (C) and defection (D), for reasons that shall soon become apparent.

Table 1: A summary of payoff matrices with Nash equilibrium (NE) and Pareto optimal (PO) results for various classical games

Game	*Payoff matrix*		*NE payoffs*	*PO payoffs*	*Condition*	*Preferred strategy*	(a, b, c, d)
Chiken	(b, b) (a, c)	(c, a) (d, d)	$(a, c) \vee (c, a)$	(b, b)	$2b > a + c$	*opposite of opponent*	$(4, 3, 1, 0)$
Prisoner's Dilemma	(b, b) (a, d)	(d, a) (c, c)	(c, c)	(b, b)	$2b > a + d$	D	$(5, 3, 2, 1)$
Deadlock	(c, c) (a, d)	(d, a) (b, b)	(b, b)	(b, b)	$2b > a + d$	D	$(3, 2, 1, 0)$
Stag hunt	(a, a) (b, d)	(d, b) (c, c)	$(a, a) \vee (c, c)$	(a, a)	–	C	$(3, 2, 1, 0)$
Battle of the sexes	(a, b) (c, c)	(c, c) (b, a)	$(a, b) \vee (b, a)$	$(a, b) \vee (b, a)$	–	*same as opponent*	$(2, 1, 0)$

With a sufficient *degree of entanglement*, the quantum player in a classical-quantum two player game can use the extra possibilities available to help steer the game towards their most desired result, giving a payoff above that achievable by classical strategies alone. There are critical values of the entanglement parameter γbelow (or occasionally above) which it is no longer an advantage to have access to quantum moves. That is, where the quantum player can no longer outscore his/her classical NE result. These represent a phase change in the classical- quantum game where a switch between the quantum miracles move and the dominant classical strategy is warranted. With typical values for the payoffs and a classical player opting for his/her best strategy, the critical value for $\sin\gamma$ is $\sqrt{\frac{1}{3}}$ for chicken, $\sqrt{\frac{1}{5}}$ for Prisoner's dilemma and $\sqrt{\frac{2}{3}}$ for deadlock, while for stag hunt and the battle of the sexes there is no particular advantage to the quantum player.

Table 2: Value of $\sin\gamma$ *above which the expected value of* $\boldsymbol{B's(A's)}$ *payoff exceeds*

Game	*A's strategy*	*B's strategy*	$\langle \$_B \rangle > \langle \$_A \rangle$	$\langle \$_B \rangle > \langle \$_A \rangle\,(NE)$	$\langle \$_B \rangle > \langle \$_A \rangle\,(PO)$
Chicken	$\hat{C}$	$\hat{M}_{01}$	*always*	$< \sqrt{\frac{a+b-2c}{b-d}}$	$< \sqrt{\frac{a-b}{b-d}}$
	$\hat{D}$	$\hat{M}_{01}$	$\frac{1}{\sqrt{2}}$	$\sqrt{\frac{c-d}{a-c}}$	$\sqrt{\frac{2b-c-d}{a-c}}$
Prisoner's Dilemma	$\hat{C}$	$\hat{M}_{01}$	*always*	*always*	$\sqrt{\frac{a-b}{c-d}}$
	$\hat{D}$	$\hat{M}_{01}$	$\frac{1}{\sqrt{a-d}}$	$\sqrt{\frac{c-d}{a-d}}$	$\sqrt{\frac{2b-c-d}{a-d}}$
Deadlock	$\hat{C}$	$\hat{M}_{01}$	*always*	$\sqrt{\frac{2b-a-c}{b-c}}$	$\sqrt{\frac{2b-a-c}{b-c}}$
	$\hat{D}$	$\hat{M}_{01}$	$\frac{1}{\sqrt{2}}$	$\sqrt{\frac{b-d}{a-d}}$	$\sqrt{\frac{b-d}{a-d}}$
Stag hunt	$\hat{C}$	$\hat{M}_{00}$	$< \frac{1}{\sqrt{2}}$	$\sqrt{\frac{c-d}{a-d}}$	*never*
	$\hat{D}$	$\hat{M}_{00}$	*never*	$< \sqrt{\frac{a+b-2c}{b-d}}$	*never*
Buttle of the sexes	$\hat{O}$	$\hat{M}_{11}$	$\frac{1}{\sqrt{2}}$	$\sqrt{\frac{b-c}{a-b}}$	$\sqrt{\frac{b-c}{a-b}}$
	$\hat{T}$	$\hat{M}_{11}$	*always*	*if* $a + c > 2b$	*if* $a + c > 2b$

Remark. It has been questioned by Peres and Wootters in [25] some times ago that where more information can be extracted from a composite quantum system by performing collective measurements on the system as a whole. Several studies addressed the same question and showed that collective measurements usually provide more information than the measurements on the individual subsystems. Quantum entanglement is believed to be responsible for this.

Another question can be addressed for two composite entangled quantum subsystems **A** and **B**: Which one of the two subsystems provides more information than the other subsystem? As an example, we investigate the following quantum card game to give more insight to the question.

Example: *Quantum card game with optimal guessing strategy* [26]. Three different quantum cards, which are non-orthogonal qubits are sent to two different players, **A** and **B**, randomly. **A** receives one of the three cards, and **B** receives the remaining two cards form a card dealer. In this game **B** could know better than **A** does on guessing **A**'s card, no matter what **B** chooses to measure his two cards collectively or separately.

B's best strategy for guessing **A**'s card is to measure his two cards collectively.

Physical interpretation of game model. The dealer shuffles three quantum cards randomly and then sends **A** one of the cards. **B** then receives the remaining two cards from the dealer. In the classical world, the three cards are actually orthogonal to each others and thus are totally distinguishable. Therefore, **A** knows her card with 100% confidence, and **B** also knows **A**'s card with 100% confidence by simply looking at his two cards. In the quantum world, the three cards can be viewed as three qubits and are in general non-orthogonal to each other. The non-orthogonal forces both **A** and **B** to do measurements on their cards and then make guesses. Formally, the game has two players, **A** and **B**, and one card dealer. The dealer holds three quantum cards, which are non-orthogonal spin-$\frac{1}{2}$particles ensemble

$$\left\{ |\psi_1\rangle = (1,0)\,, |\psi_2\rangle = \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right), |\psi_3\rangle = \left(-\frac{1}{2}, \frac{\sqrt{3}}{2}\right) \right\},$$

respectively. In the beginning of the game, the dealer shuffles the cards randomly and gives **A** one of the cards. **B** picks the remaining two cards from the dealer. **A** and **B** does not have the possibility of communication on this step. Both player's then make own guesses on what card is in **A**'s hand. After making their guesses, the dealer will check their answer and decide who the winner of the game is. Based upon the game description, we can view the dealer's cards as a composite quantum system, described by density (matrix) function ρ and both **A**'s card and **B**'s cards as two subsystems, ρ_A andρ_B, of the composite system.

$$\begin{array}{ll}
\textit{Composite system}, \rho & \frac{1}{6}\left\{ \begin{array}{l} |\psi_1\rangle\langle\psi_1|_A \otimes |\psi_2\psi_3\rangle\langle\psi_2\psi_3|_B + |\psi_1\rangle\langle\psi_1|_A \otimes |\psi_3\psi_2\rangle\langle\psi_3\psi_2|_B \\ + |\psi_2\rangle\langle\psi_2|_A \otimes |\psi_1\psi_3\rangle\langle\psi_1\psi_3|_B + |\psi_2\rangle\langle\psi_2|_A \otimes |\psi_3\psi_1\rangle\langle\psi_3\psi_1|_B \\ + |\psi_3\rangle\langle\psi_3|_A \otimes |\psi_1\psi_2\rangle\langle\psi_1\psi_2|_B + |\psi_3\rangle\langle\psi_3|_A \otimes |\psi_2\psi_1\rangle\langle\psi_2\psi_1|_B \end{array} \right\} \\
\textit{Subsystem}, \rho_A \equiv Tr_B(\rho) & \frac{1}{3}\left[|\psi_1\rangle\langle\psi_1|_A + |\psi_2\rangle\langle\psi_2|_A + |\psi_3\rangle\langle\psi_3|_A\right] = diag\left(\frac{1}{2}, \frac{1}{2}\right) \\
\textit{Subsystem}, \rho_B \equiv Tr_B(\rho) & \frac{1}{6}\left\{ \begin{array}{l} |\psi_1\psi_2\rangle\langle\psi_1\psi_2|_B + |\psi_2\psi_1\rangle\langle\psi_2\psi_1|_B + |\psi_1\psi_3\rangle\langle\psi_1\psi_3|_B \\ + |\psi_3\psi_1\rangle\langle\psi_3\psi_1|_B + |\psi_2\psi_3\rangle\langle\psi_2\psi_3|_B + |\psi_3\psi_2\rangle\langle\psi_3\psi_2|_B \end{array} \right\}
\end{array}$$

As above mentioned in the classical world, all cards are orthogonal to each and thus totally distinguishable. That is, both **A** and **B** posses the same information on **A**'s card: **A** knows exactly what her card is by simply looking at the card she has, **B** also concludes on what **A** has in hand by simply looking at two cards. Therefore, it is

not likely for them to gamble. In the quantum world, the non-orthogonal nature of cards takes parts in this game: the quantum cards are no longer totally distinguishable. Therefore, the game becomes uncertain and the gambling between **A** and **B** is possible: **A** no longer determines what she has in hand with 100% certainty and so does **B**. If **A** performs measurement on her card along the direction $|\phi_\alpha\rangle = (cos\,\alpha, sin\,\alpha)$ (Stern-Gerlach measurement), she would obtain the spin-up (or spin-down) result with the following probabilities:$P(up) = Tr\{|\phi_\alpha\rangle\langle\phi_\alpha|\rho_A\}$; $P(down) = 1 - P(up)$.In the game considered, A always measures the spin-up or spin-down outcomes with equal probabilities, $P(up) = P(down) = \frac{1}{2}$;

no matter what the measuring direction $|\phi_\alpha\rangle$ is. As shown in Table 2, when the outcome r is obtained after the measurement, **A** knows *a posteriori* the probability $P(i|r)$ for preparation$|\psi_i\rangle$.

A simply cannot determine what her card is with 100% certainty.

The optimal strategy probability of **A**'s. The optimal probability can be obtained minimizing Shannon entropy. Player **A** has three strategies: $\{|\psi_3\rangle, |\psi_2\rangle, |\psi_2\rangle \vee |\psi_3\rangle\}$. The first strategy is to guess $|\psi_3\rangle$ for$0 < \alpha \leqslant \frac{\pi}{6}$. For example, **A** can choose the first strategy to guess her card. When the measurement outcome in spin-up, **A** will guess her card successfully with probability $\frac{2}{3}\cos^2\alpha$ (see Table 2), and make a wrong guess with probability$\left(1 - \frac{2}{3}\cos^2\alpha\right)$. When the measurement outcome in spin-down, she guess the card successfully with probability $\frac{2}{3}\sin^2\left(\alpha + \frac{\pi}{3}\right)$ and guess it wrong with probability $\left(1 - \frac{2}{3}\sin^2\left(\alpha + \frac{\pi}{3}\right)\right)$ (see, Table 3).

Table 3: Conditional probabilities for **A***'s measurement outcomes*

Position	$P(1\|r)$	$P(2\|r)$	$P(3\|r)$
$Spin - up$	$\frac{2}{3}\cos^2\alpha$	$\frac{2}{3}\cos^2\left(\alpha - \frac{\pi}{3}\right)$	$\frac{2}{3}\cos^2\left(\alpha + \frac{\pi}{3}\right)$
$Spin - down$	$\frac{2}{3}\sin^2\alpha$	$\frac{2}{3}\sin^2\left(\alpha - \frac{\pi}{3}\right)$	$\frac{2}{3}\sin^2\left(\alpha + \frac{\pi}{3}\right)$

Thus the Shannon entropy S^{Sh} for the "success – failure" binary information is as following$\left(P(r) = \frac{1}{3}\cos^2\alpha\right)$:

$$\begin{aligned} S^{Sh} &= -\sum_r P(r)\{P(success|r)\log P(success|r) + P(failure|r)\log P(failure|r)\} \\ &= -\left(\tfrac{1}{3}\cos^2\alpha\right)\log\left(\tfrac{2}{3}\cos^2\alpha\right) - \left(\tfrac{1}{2} - \tfrac{1}{3}\cos^2\alpha\right)\log\left(1 - \tfrac{1}{3}\cos^2\alpha\right) \\ &\quad -\tfrac{1}{3}\sin^2\left(\alpha + \tfrac{\pi}{3}\right)\log\left(\tfrac{2}{3}\sin^2\left(\alpha + \tfrac{\pi}{3}\right)\right) - \left(\tfrac{1}{2} - \tfrac{1}{3}\sin^2\alpha\right)\log\left(1 - \tfrac{2}{3}\sin^2\alpha\right) \end{aligned}$$

The minimum of the entropy S^{Sh} occurs at $\alpha = \frac{\pi}{12}$ for$0 < \alpha \leqslant \frac{\pi}{6}$. In thus leads to the successful guessing probability for **A**:$P(success) = \frac{1}{3}\left\{\cos^2\alpha + \sin^2\left(\alpha + \frac{\pi}{3}\right)\right\}$. When$\alpha = \frac{\pi}{12}$, the first strategy has an optimal value $P(success) = \frac{2+\sqrt{3}}{6} \cong 0.622$. Second strategy is guessing $|\psi_2\rangle$for $-\frac{\pi}{6} \leqslant \alpha < 0$. This one has the same optimal guessing probability as the first strategy at$\alpha = -\frac{\pi}{12}$. The third strategy is to guess randomly $|\psi_2\rangle$ or $|\psi_3\rangle$ with equal probability for $\alpha = 0$.

This strategy is not optimal simply because it has a smaller successful probability of guessing.

The optimal strategies for **B** *player.* **B** receives two cards from the dealer. **B** knows that there are six possible combinations for his cards. They are as following:

$$\begin{array}{llllll} |A\rangle = |\psi_1\psi_2\rangle & |B\rangle = |\psi_2\psi_3\rangle & |C\rangle = |\psi_3\psi_1\rangle \\ |A'\rangle = |\psi_2\psi_1\rangle & |B'\rangle = |\psi_3\psi_2\rangle & |C'\rangle = |\psi_1\psi_3\rangle \end{array}$$

These six states are not orthogonal states. That means **B** has no way of distinguishing them with 100% certainty. However, **B** does not really need to know exactly what

he has in hand to infer **A**'s card. For example, **B** will infer that **A**'s card is $|\psi_3\rangle$ if he thinks he has $|A\rangle$ or $|A'\rangle$ in hand. If **B** has $|B\rangle$ or$|B'\rangle$, then he will infer $|\psi_1\rangle$ for **A**'s card. Similarly, if **B** has $|C\rangle$ or $|C'\rangle$, then he will think that **A** has the $|\psi_2\rangle$ card in hand. To make a reasonable guess, **B** needs to measure his cards before guessing. There are two kinds of the measuring methods: (i) Measure them collectively; or (ii) Measure the two cards one by one.

Let us consider both possibilities.

Case (i): C*ombined measurement on* **B***'s cards.* Since the dimension of the Hilbert space for **B**'s cards is four, **B** needs to choose according to quantum mechanics laws a suitable orthonormal basis $\{|\phi_i\rangle, i = 1.2, 3, 4\}$ in the Hilbert space for his measurement:

$$|\phi_i\rangle = \sum_{i=1}^{4} j_i |J_i\rangle, \ j = a, b, c, d; \ J = A, B. C. D.$$

For example, for$j = a$, $J = A$: $|\phi_1\rangle = a_1 |A_1\rangle + a_2 |A_2\rangle + a_3 |A_3\rangle + a_4 |A_4\rangle$, where the base vector $|\phi_1\rangle$ is written in terms of other orthonormal bases $\{|A_i\rangle\}$in the Hilbert space, respectively

$$|A_1\rangle = \sqrt{\frac{2}{5}} (|A\rangle + |A'\rangle) \qquad |A_3\rangle = \sqrt{\frac{2}{3}} (|\psi_1, \psi_2\rangle - |\psi_2, \psi_3\rangle)$$

Similarly another representations of$|\phi_i\rangle$, $i = 2, 3, 4$ are described in [26]. The unknown coefficients a_i should be determined by the optimal guessing strategies and are assumed to be real numbers for simplicity with the following orthonormal conditions: $\sum_{k=1}^{4} a_k^2 = 1$. Any measurement M along the $|\phi_4\rangle$ direction can be related to the measurements along other directions,

$$Tr\{|\phi_4\rangle \langle\phi_4| M\} = Tr(M) - \sum_{k=1}^{3} Tr\{|\phi_k\rangle \langle\phi_k| M\}.$$

With orthonormal measuring basis, **B** makes the following guessing strategy: (i) Guess $|\psi_3\rangle$, $|\psi_2\rangle$ or $|\psi_2\rangle$ for **A**'s card when the measurement outcome is $|\phi_1\rangle, |\phi_2\rangle$ or $|\phi_3\rangle$, respectively; (ii) When the outcome is $|\phi_4\rangle$, **B** has three choices in general: 1) Guess one of the three cards for **A**; for example, guess $|\psi_3\rangle$ for **A**; (iii) Guess **A**'s card randomly from two of the three possible card; for example, randomly guess $|\psi_3\rangle$ or $|\psi_1\rangle$; (iv) Make a random guess from the three cards.

In general, different guessing choices for the outcome $|\psi_4\rangle$may lead to different optimal guessing probabilities. However, numerical study shows [1] that all these three choices have the same optimal guessing probabilities, which correspond to the same measuring basis.

Therefore, we can discuss only the third guessing choices. With the guessing strategy, **B** knows that the probability for a successful guessing on **A**'s card is P_B (combined) is following:

$$\begin{aligned} P_B(combined) &= \frac{1}{6}\left\{\begin{array}{l}\langle A|\phi_1\rangle^2 + \langle A'|\phi_1\rangle^2 + \langle B|\phi_2\rangle^2 + \langle B'|\phi_2\rangle^2 + \langle C|\phi_3\rangle^2 + \langle C'|\phi_3\rangle^2 \\ + \frac{1}{3}\left[\langle A|\phi_4\rangle^2 + \langle A'|\phi_4\rangle^2 + \langle B|\phi_4\rangle^2 + \langle B'|\phi_4\rangle^2 + \langle C|\phi_4\rangle^2 + \langle C'|\phi_4\rangle^2\right]\end{array}\right\} \\ &= \frac{1}{3} + \frac{2}{15}\left(a_1^2 + b_1^2 + c_1^2\right) - \frac{1}{12}\left(a_3^2 + b_3^2 + c_3^2\right) - \frac{1}{20}\left(a_4^2 + b_4^2 + c_4^2\right) \\ &\quad + \frac{1}{30}\left(a_1 a_4 + b_1 b_4 - c_1 c_4\right) \end{aligned}$$

When $a_1 = b_1 = c_1 = \frac{4+\sqrt{2}}{\sqrt{30}}$, $a_2 = b_2 = c_2 = 0$, $a_3 = b_3 = c_3 = 0$and$a_4 = b_4 = c_4 = \frac{2-\sqrt{2}}{\sqrt{15}}$,the successful probability $P_B\,(combined)$ has a maximally value $P_B\,(combined) = \frac{3+\sqrt{2}}{6} \cong 0.7357$.

For the second method (individual measure the two cards on by one), **B** will measure his first card correctly with the optimal probability$P_1 = \frac{2+\sqrt{3}}{6}$. The second card then can be measured correctly with the optimal probability$P_1 = \frac{2+\sqrt{3}}{4}$. Thus **B** can know his cards exactly with the optimal probability P_{12} as following: $P_{12} = P_1 \cdot P_2 = \frac{7+4\sqrt{3}}{24} \cong 0.5803$.

Remark. However, except for measuring his cards successfully **B** can also infer the same card for **A** by making two consecutive incorrect guesses on his cards. For example, assume that **B** does receive$|\psi_3\,\psi_2\rangle$, he still infer the same result $|\psi_1\rangle$ for **A**. For this case, the probability of a successful guess is $P_{12} = \left(1 - \frac{2+\sqrt{3}}{6}\right) \cdot \frac{1}{2} \cdot \frac{1}{2} = \frac{4-\sqrt{3}}{24}$. Therefore, the optimal probability that **B** will infer the correct card **A** is $P_B\,(separate)$is as following:

$$P_B\,(separate) = P_{12} + P_{21} = \frac{11+3\sqrt{3}}{24} \cong 0.6748 > 0.622.$$

Thus, the best guessing strategy for **B** to know **A**'s card is doing combined (collective) measurement on his cards. Therefore, the non-orthogonally forces both **A** and **B** to do measurements on their cards and then make their guesses. The best chance for **A** to know her card is $P_A \cong 0.622$, a probability, which is nearly doubled than a random guess $P = \frac{1}{3}$. On the other hand, **B** can choose either to measure his cards by one or two measure them collectively. Both ways a measuring all give **B** the optimal guessing probabilities $P_B\,(separate) \cong 0.6741$ and $P_B\,(combined) \cong 0.7357$ which are larger than **A**'s optimal guessing probability. That is, **B** has a higher winning probability than **A** does in the quantum guessing game. Let us consider entanglement-free quantum algorithms and the role of *interference* in these processes.

3. Entanglement-free quantum algorithms and strategies without entanglement

There can be exists quantum computational speed-up without entanglement when we use the mutual computational process as "*soft computing optimization – quantum optimization*" for design process of robust KB-FC. We briefly describe the entanglement-free quantum speed-up algorithm and application of simulation results in robust KB-FC design process.

3.1 The Entanglement-free quantum efficient algorithm

Let us state the following **Problem** (*Mosca*, 2000): *Given an integer N function* $f : x \to m\,x + b$, *where* $x, m, b \in \mathbb{Z}_N$, *find* m. The classical analysis reveals that no information about m can be obtained with only one evolution of the function$f$. Conversely, given the unitary operator U_f acting in a reversible way in the Hilbert space $\mathcal{H}_N \otimes \mathcal{H}_N$ such that:

$$U_f\,|x\rangle\,|y\rangle = |x\rangle\,|y \oplus f\,(x)\rangle\,, \tag{4}$$

(where the sum is to be interpreted as modulus N), there is a QA solving this problem with only one query to U_f.

Quantum algorithm structure. Let us take $N = 2^n$. being n the number of qubits. The QA efficiently solving the problem previously presented reads as follows:

Step	Computational algorithm
1	Prepare two registers of n qubits in the state $\|0\ldots0\rangle\|\psi_1\rangle \in \mathrm{H}_N \otimes \mathrm{H}_N$, where $\|\psi_1\rangle = QFT(N)^{-1}\|1\rangle$, and $QFT(N)^{-1}$ denotes the inverse quantum Fourier transform in a Hilbert space of dimension N
2	Apply $QFT(N)$ over the first register
3	Apply U_f over the whole quantum state
4	Apply $QFT(N)^{-1}$ over the first register
5	Measure the first register and output the measured value

We now show (according to [27]) how the proposed QA leads to the solution of the problem. The analysis raises two observations concerning the way both entanglement and *majorization* behave in the computational process:

1. In the first step of the algorithm, the quantum state is separable, noting that the QFT (and its inverse) applied on a well-defined state in the computational basis leads to a perfectly separable state. Actually, this separability holds also step-by-step when the decomposition for the QFT is considered, such as the Coppersmith's decomposition. That is, the quantum state $|0\ldots0\rangle\,|\psi_1\rangle$ is unentangled.

2. The second step of the algorithm corresponds to a QFT in the first register. This action leads to a step-by-step *minorization* of the probability distribution of the possible outcomes while it does not use neither create any entanglement. Moreover, *natural minorization* is at work due to the absence of *interference* terms.

3. Next, it is easy to verify that the quantum state

$$|\psi_1\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{-2\pi i \frac{j}{N}} |j\rangle \tag{5}$$

is an eigenstate of the operator $|y\rangle \rightarrow |y + f(x)\rangle$ with eigenvalue $e^{2\pi i \frac{f(x)}{N}}$.

Remark. After the third step, the quantum state reads

$$\frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi i \frac{f(x)}{N}} |\psi_1\rangle = \frac{e^{2\pi i \frac{b}{N}}}{\sqrt{N}} \underbrace{\left(\sum_{x=0}^{N-1} e^{2\pi i \frac{m_x}{N}} \right)}_{\boxed{First\ Register}} |\psi_1\rangle \tag{6}$$

The probability distribution of possible outcomes has not been modified, thus not affecting majorization. Furthermore, the pure quantum state of the first register in Eq.(6) can be written as $QFT(N)|m\rangle$ (up to a phase factor), so this step has not created any entanglement among the qubits of the system either.

4. In the fourth step of the algorithm, the action of the operator $QFT(N)^{-1}$ over the first register as interference operation leads to the state$e^{2\pi i \frac{b}{N}}|m\rangle|\psi_1\rangle$.

5. A subsequent measurement in the computational basis over the first register provides the desired solution. (Recalling the results from [20], we see that the inverse QFT naturally majorizes step-by-step the probability distribution attached to the different outputs).

On the other hand, the separability of the quantum state still holds step-by-step.

Remark. It is clear that the QA is more efficient than any of its possible classical counterparts, as it only needs of a single query to the unitary operator U_f to get the solution. We can summarize this analysis of majorization for present QA as follows: The entanglement-free efficient QA for finding a hidden affine function shows a majorization cycle based on the action of $QFT(N)$ and $QFT(N)^{-1}$. It follows that there can exist quantum computational speed-up without the use of entanglement. In this case, it is seen that no resource increases exponentially. Yet, a majorization cycle is present in the process, which is rooted in the structure of both the QFT and the quantum state.

3.2 Classical-quantum strategy without entanglement

Quantum mechanics affects game theory: for certain games a suitable quantum strategy is able to beat any classical strategy. Let us now discuss the possibility to design quantum strategies without entanglement using two simple examples of entanglement-free games: **PQ**-game [28] and card game [29].

Quantum and classical game strategies: **PQ**-*game example.* Let us consider as example, the penny flipping game (**PQ** *PENNY FLIP* game [28]). The game is penny flipping, where player **P** places a penny head up in a box, after which player **Q**, then player **P**, and finally player **Q** again, can choose to flip the coin or not, but without being able to see it. If the coin ends up being head up, player **Q** wins, else player **P** wins. The winning (or cheating, depending upon one's perspective) quantum strategy of **Q** now consists of putting the penny into superposition of head up and down. Since player **P** is allowed to interchange only up and down he is obviously not able to change that superposition, so that **Q** wins the game by rotating the penny back to its initial state.

Physical interpretation of **PQ**-*game.* **Q** produces a penny and asks **P** to place it in a small box, head up. Then **Q**, followed by **P**, followed by **Q**, reaches into box, without looking at the penny, and either flips it over or leaves it as it is. After **Q**'s second turn they open the box and **Q** wins if the penny is head up. **Q** wins every time they play, using the following quantum game gate:

$$|\psi_{fin}\rangle = \boxed{\underbrace{H}_{Q\ strategy} \cdot \underbrace{\sigma_x(I_2)}_{P\ strategy} \cdot \underbrace{H}_{Q\ strategy}} \underbrace{|0\rangle}_{Initial\ state}$$

and the following quantum strategy [28]:

Initial state and strategy	Player strategy	Result of operation
$\|0\rangle$	$\xrightarrow[H]{Q}$	$\frac{1}{\sqrt{2}}(\|0\rangle+\|1\rangle)$
-	$\xrightarrow[\sigma_x(\text{or } I_2)]{P}$	$\frac{1}{\sqrt{2}}(\|1\rangle+\|0\rangle)$ or $\frac{1}{\sqrt{2}}(\|0\rangle+\|1\rangle)$
-	$\xrightarrow[H]{Q}$	$\|0\rangle$

Here 0 denotes "head" and 1 denotes "tail", and $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \equiv NOT$ implements **P**'s possible action of flipping the penny over. **Q**'s quantum strategy of putting the penny into the equal superposition of "head" and "tail" on his first turn means that whether **P** flips the penny over or not, it remains in an equal superposition which **Q** rotates back to "head" by applying Hadamard transformation Hagain since $H = H^{-1}$ and $\frac{1}{\sqrt{2}}(|1\rangle + |0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. After measurement **Q** received the state the state$|0\rangle$. The second application of Hadamard transformation plays the role of *constructive interference*. So when they open the box, **Q** always wins *without* using of *entanglement*.

Remark. If **Q** were restricted to playing classically, i.e., to implementing only σ_x or I_2 on his turns, an optimal strategy for both players would be to flip the penny over or not with equal probability on each turn. In this case **Q** would win only half time, so he does substantially better by playing quantum mechanically.

Let us consider the interesting case of classical-quantum card game without entanglement. In the classical game, one player **A** can always win with the probability$\frac{2}{3}$. But if the other player **B** performs quantum strategy, he can increase his winning probability from $\frac{1}{3}$ to$\frac{1}{2}$. In this case **B** is allowed to apply quantum strategy and the original unfair game turns into a fair and zero-sum game, i.e., the unfair classical game becomes fair in quantum world. In addition, this strategy does *not use entanglement*, which is different from most of above described works in [1].

Game (see Table 1 in [1]): *Classical-quantum card game with quantum strategy without entanglement.* We will discuss two-player card game [29].

Classical game model. The classical model of card game is explained as following. **A** has three cards. The first card has one circle in its both sides, the second has one dot in its both sides and the third card has one circle in one side and one dot in the other. At first step, **A** put the three cards into black box. The cards are randomly placed in the box after **A** shakes it. Both players cannot see what happens in the box. At second step **B** take one card from the box without flipping it. Both players can only see the upper side of the card. **A** wins one coin if the pattern of the down side is the same as that of the upper side and lose one coin when the patterns are different. It is obvious that **A** has $\frac{2}{3}$probability to win and **B** only has$\frac{1}{3}$. **B** is in a disadvantageous situation and the game is unfair to him. Any rational player will not play the game with **A** because the game is unfair. In order to attract **B** to play with him, before the original second step **A** allows **B** to have one chance to operate on the cards. That is **B** has one step query on the box. In the classical world, **B** can only attain one card information after the query. Because the card is in the box, so what **B** knows is only one upper side pattern of the three cards. Except this he knows nothing about the three cards in the black box. So in the classical field even having this one step query, **B** still will be in disadvantageous state and the game is still unfair. Let us consider the quantized approach to this game.

The quantized card game. When we investigate the game in the quantum field, the whole thing is changed. We will see that the game turns into a fair zero-sum game and

both players are in equal situation. Let us consider the case when **A** use the classical strategy and **B** use the quantum strategy. In the first step, **A** puts the cards in the box and shakes the box that is she prepares the initial state randomly.

We describe the card state be $|0\rangle$if the pattern in the upper side is circle and $|1\rangle$if it is dot.

So the upper sides of the three cards in the box be described as$|r\rangle = |r_0\rangle\,|r_1\rangle\,|r_2\rangle$, where $r_0, r_1, r_2 \in \{0,1\}$, which means $|r_0\rangle, |r_1\rangle, |r_2\rangle$ are all eigenstates other superposition of $|0\rangle$ and $|1\rangle$.

Remark. After the first step of the game, **A** gives the black box to **B**. Because **A** thinks in *classical* way, in her mind **B** cannot get information about all upper side patterns of the three cards in the box. So **A** can still win with higher probability. But what **B** use is *quantum* strategy: He replaces the classical one step query with one step quantum query. The following shows how **B** query the box.

Algorithm. Let us that **B** has a quantum machine that applies an unitary operator Uon its three input qubits and give three output qubits. This machine depends on the state $|r\rangle$ in the box that **A** gives **B**. The explicit expression of $U$and its relation with $|r\rangle$ is as following $U = U_0 \otimes U_1 \otimes U_2$ where$U_k = \begin{cases} I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & if\ r_k = 0 \\ \sigma_x = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} if\ r_k = 1 \end{cases} =$

$\begin{pmatrix} 1 & 0 \\ 0 & \exp\{i\pi r_k\} \end{pmatrix}$.

The processing of query is shown in Figure 2.

After the process, the output state is

$$|\psi_{fin}\rangle = (H \otimes H \otimes H)\,U\,(H \otimes H \otimes H)\,|000\rangle = (HU_0H)\,|0\rangle\,(HU_1H)\,|0\rangle\,(HU_2H)\,|0\rangle\,.$$

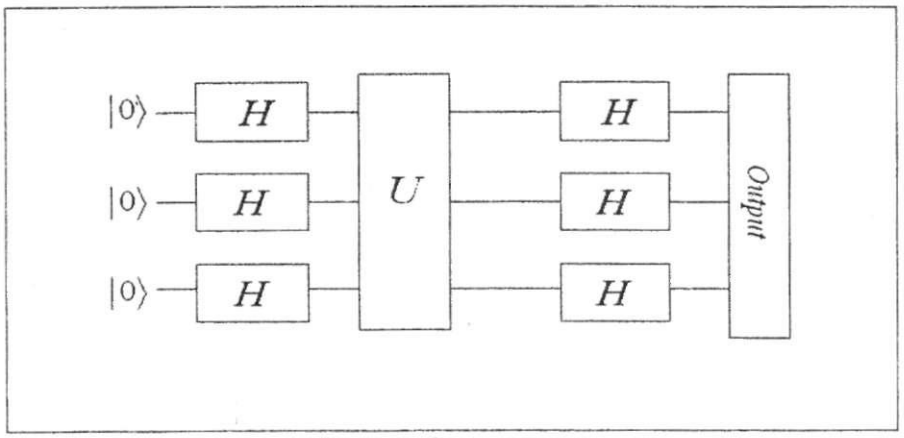


Figure 2: Query processing

Because

$$HU_kH = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi r_k} \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1+e^{i\pi r_k} & 1-e^{i\pi r_k} \\ 1-e^{i\pi r_k} & 1+e^{i\pi r_k} \end{pmatrix}.$$

So

$$HU_kH\,|0\rangle = \frac{1+e^{i\pi r_k}}{2}\,|0\rangle + \frac{1-e^{i\pi r_k}}{2}\,|1\rangle = \begin{cases} |0\rangle & if\ r_k = 0 \\ |1\rangle & if\ r_k = 1 \end{cases} = |r_k\rangle$$

From above, it is obvious to see that **B** can obtain the complete information about the upper patterns of all the three cards through one query. There are only two possible

kinds of output states in the black box, which is $|0\rangle|0\rangle|1\rangle$ or$|1\rangle|1\rangle|0\rangle$, that is two circles and one dot in the upper side or two dots and one circle. Let us assume that the states of the cards after first step is two circles and one dot, i.e.,$|0\rangle|0\rangle|1\rangle$. After one step query, **B** knows the complete information about the upper patterns, but he has no individual information about which upper pattern corresponding to which card. Then he takes one card out of the box and to see what pattern is in the upper side. If **B** finds out that he is in disadvantage situation, the upper pattern of the card is dot ($|1\rangle$), he refuses to play with **A** in this turn because he knows the down side is dot definitely. Otherwise if the upper side pattern is circle ($|0\rangle$), then he knows that the down side pattern is circle $|0\rangle$ or dot$|1\rangle$. So he continues this turn because he has the probability $1/2$ to win. **B** will continue the game because he has probability $\frac{1}{2}$ to win. Hence the game becomes fair and is also zero-sum.

Entanglement-free algorithm game. One of the reason why the quantum strategies in games are better than classical strategies is that the initial state is maximal entangled. The quantum strategy in card game applied by **B** includes *no entanglement* and is still better than classical strategy. The initial state input the quantum machine is $|0\rangle|0\rangle|0\rangle$ which is obviously separable. After the Hadamard transformation, the state is$\frac{1}{\sqrt{2^3}}(|0\rangle+|1\rangle)\otimes(|0\rangle+|1\rangle)\otimes(|0\rangle+|1\rangle)$. Performed by U, the state becomes $\frac{1}{\sqrt{2^3}}\left(|0\rangle+e^{i\pi r_0}|1\rangle\right)\otimes\left(|0\rangle+e^{i\pi r_1}|1\rangle\right)\otimes\left(|0\rangle+e^{i\pi r_2}|1\rangle\right)$. And the states, after the second Hadamard transformation, are the output state$|r_0\rangle|r_1\rangle|r_2\rangle$. In the whole procedure, the state is tensor products of the states of the individual qubits, so it is unentangled. And because the operators (H and$U$) are also tensor product of the individual local operators on these qubits, so it is obviously that in this quantum game there is no entanglement applied.

Remark. Entanglement is important for static games (such as Prisoner's Dilemma) but may be not necessary in dynamic games (such as the PQ-game and the card game). In static games, each player can only control his qubit and his operation is local. So in classical world, the operation of one player cannot have influence on others in the operational process. But in quantum field, through entanglement the strategy changing of one player could influent not only himself but also his opponents. In dynamic games, players can control all qubits at any step. So just like quantum algorithms [30], in dynamic games players can use quantum strategies without entanglement to solve problem, even entangled quantum strategies could be re-described with other quantum strategies without entanglement.

Thus, if **B** is given quantum strategy – one step quantum query – against his classical opponent **A**, she cannot always win with high probability. Both players are in equal situation and the game is a fair zero-sum game. The quantum game includes no entanglement and quantum-over-classical strategy is achieved using only *interference*. Quantum strategy could be still powerful without entanglement like in quantum information and algorithm [31].

3.3 General form of dynamic PQ-game and quantum strategies definition: Interrelations with quantum algorithms

In general case the game can be described as in the following table.

Remark. Since only **P** and **Q** play, these are two-player games; they are zero-sum since when **Q** wins, **P** loses, and *vice versa*. A pure quantum strategy for **Q** is a sequence$u_i \in Q_i$. A pure (classical) strategy for **P** is a sequence$s_i \in P_i$, while a mixed (classical) strategy for **P** is a sequence of probability distributions$f_i : P_i \to [0,1]$. If

both **Q** and **P** play pure strategies, the corresponding evolution of the **PQ**-game is described by quantum game gate$|\psi_{fin}\rangle = \prod_k u_{k+1} s_k u_k |\psi_{in}\rangle$.

Definition	Main operations
(i)	A Hilbert space H (the possible states of the game) with $N = \dim \mathrm{H}$
(ii)	An initial state $\psi_0 \in \mathrm{H}$
(iii)	Subset $Q_i \subset U(N), i \in \{1,\ldots,k+1\}$ - the elements of Q_i are the moves **Q** chooses among on turn i
(iv)	Subset $P_i \subset S_N, i \in \{1,\ldots,k\}$, where S_N is the permutation group on N elements - the elements of P_i are the moves **P** chooses among on turn i
(v)	A projection operator Π on H (the subspace W_Q fixed by Π consists of the winning states for **Q**)

Quantum measurement. After **Q**'s last move the state of the game is measured withΠ. According to the rules of quantum mechanics, the players observe the eigenvalue 1 with probability $Tr\left(\psi^{\dagger}\Pi\psi\right)$; this is the probability that the state is projected into W_Q and **Q** wins. More generally, if **P** plays a mixed strategy, the corresponding evolution of the **PQ**-game is described by

$$\rho_f = u_{k+1}\left(\sum_{s_k \in P_k} f_k(s_k)\, s_k u_k \ldots u_2\left(\sum_{s_1 \in P_1} f_1(s_1)\, s_1 u_1 \rho_0 u_1^{\dagger} s_1^{\dagger}\right) u_2^{\dagger} \ldots u_k^{\dagger} s_k^{\dagger}\right) u_{k+1}^{\dagger},$$

where$\rho_0 = |\psi_0\rangle \otimes \left\langle \psi_0^{\dagger}\right|$. Again, after **Q**'s last move ρ_f is measured withΠ; the probability that ρ_f is projected into $W_Q \otimes W_Q^{\dagger}$ and **Q** wins is$Tr\left(\Pi\rho_f\right)$.

Remark. An equilibrium state is a pair of strategies, one for **P** and one for **Q**, such that neither player can improve his probability of winning by changing his strategy while the other does not. In general, unlike the simple case of **PQ**-game, $W_Q = W_Q(\{s_i\})$or$W_Q = W_Q(\{f_i\})$, i.e., the conditions for **Q**'s win can depend on **P**'s strategy. There are with mixed/quantum equilibria at which **Q** does better than he would at any mixed/mixed equilibrium; there are some QAs, which outperform classical ones. Let us now consider the interrelations between QAs and quantum games structures.

A QA for an oracle problem can be understood as a *quantum strategy* for a player in a two-player zero-sum game in which the other player is constrained to play *classically.* This correspondence can be formalized and we will give examples of games (and hence oracle problems) for which the quantum player can do better than that would be possible classically. In general case entanglement (or some replacement resource) is required. Surprising observation that efficient quantum search of a "sophisticated" database requires no entanglement at any time step: a quantum-over-classical reduction in the number of queries is achieved using only interference, not entanglement, within the usual model of quantum computation [31].

Quantum oracle models and reduction of query number. The problem, which forms the context for discussion is database search – identify a specific record in a large database. Formally, we label the records $\{0, 1, \ldots, N-1\}$where, for convenience when we write the numbers in binary, we take $N = 2^n$ for n a positive integer. In quantum

search are considered databases which, when queried about a specific number, respond only that the guess is correct or not. On a classical reversible computer we can implement a query by a pair of register(x, b), where x is an n-bit string representing the guess, and b is a single bit which the database will use to respond to the query. If the guess is correct, the database responds by adding 1 $(mod 2)$ to$b$: if it is incorrect, it adds 0 to b. That is, the response of the database is the operation:$|x\rangle\,|b\rangle \rightarrow |x\rangle\,|b \oplus f_a(x)\rangle$, where $f_a(x) = 1$ when $x = a$, 0 otherwise. Thus if b changes, we know that the guess is correct. Classically, it takes $N-1$ queries to solve this problem with probability 1.

Remark. The following oracles are defined in Table 4 for a general function f : $\{0,1\}^m \rightarrow \{0,1\}^n$.

Table 4: Oracles functions

Number	Title of oracle	Type	Definition
1	The *phase* oracle	P_f	$\|x\rangle\|b\rangle \rightarrow \exp\left\{\frac{2\pi i f(x)\cdot b}{2^n}\right\}\|x\rangle\|b\rangle$
2	The *standard* oracle	S_f	$\|x\rangle\|b\rangle \rightarrow \|x\rangle\|b \oplus f(x)\rangle$
3	The *minimal* (an *erasing*) oracle	M_f	$\|x\rangle \rightarrow \|f(x)\rangle$

Here x and b are strings of m and n bits respectively, $|x\rangle$ and $|b\rangle$ the corresponding computational basis states, and $\oplus$ is addition modulo2^n.

The oracles P_f and S_f are equivalent in power: each can be constructed by a quantum circuit containing just one copy of the other. If we take $m = n$and suppose we know f is a permutation on the set $\{0,1\}^n$ then M_f is a simple invertible quantum map associated to$f$. Intuitively erasing oracles seem at least as strong as standard ones, though it is not clear how to simulate the latter with the former without also having access to an oracle that map $|x\rangle$ to$|f^{-1}(x)\rangle$. One-way functions provide a clue: if f is one-way, then (by assumption) $|x\rangle\,|f(x)\rangle$ can be computed efficiently, but if $|f(x)\rangle$could be computed efficiently given $|x\rangle$ then so could $|x\rangle$ given$|f(x)\rangle$, and hence f could be inverted. For some problem, an exponential gap between query complexity given a standard oracle and query complexity given an erasing oracle [32, 33].

QAs work by supposing that they will be realized in a quantum system, which can be in a superposition of "classical" states. These states form a basis for the Hilbert space whose elements represent states of the quantum system. More generally, Grover's QSA (see in details Appendix) works with quantum queries which are linear combinations$\sum c_{x,b}\,|x,b\rangle$, where $c_{x,b}$ are complex numbers satisfying$\sum |c_{x,b}|^2 = 1$. The operations in QAs are unitary transformations, the quantum mechanical generalization of reversible classical operations. Thus the operation of the database that Grover considered is implemented on superposition of queries by a unitary transformation, which takes $|x,b\rangle$ to$|x\rangle\,|b \oplus f_a(x)\rangle$. By using $\left\lfloor \frac{\pi}{4}\sqrt{N} \right\rfloor$quantum queries, it identities the answer with probability close to 1: The final vectors for the Npossible answers a are nearly orthogonal. Let us consider one of the guessing game type that used Grover's QSA for guessing of any number between 0 and $N-1$ and to discuss the role of different quantum oracle models in the reduction of query number.

Example: *Guessing of number*. Let us suppose in PQ-game the player **Q** boats that if **P** picks any number between 0 and$N-1$, inclusive, he can guess it. **P** knows the Grover's QSA and realized that for$N=2^n$, the player **Q** can determine the number he picks with high probability by playing the following strategy:

$\|0\ldots0,0\rangle$	$\xrightarrow[H^{\otimes n}\otimes H\sigma_x]{Q}$	$\frac{1}{\sqrt{N}}\sum_{x00}^{n-1}\|x\rangle\otimes\frac{1}{\sqrt{2}}(\|0\rangle-\|1\rangle)$	$\Rightarrow$	(u_1)
	$\xrightarrow[s(f_a)]{P}$	$\frac{1}{\sqrt{N}}\sum_{x=0}^{n-1}(-1)^{\delta_{xa}}\|x\rangle\otimes\frac{1}{\sqrt{2}}(\|0\rangle-\|1\rangle)$	$\Rightarrow$	(s_1)
	$\xrightarrow[H^{\otimes n}\otimes I_2\circ s(f_0)\circ H^{\otimes n}\otimes I_2]{Q}$	$\ldots,$	$\Rightarrow$	(u_2)

using the following quantum game gate:

$$G=\left[H^{\otimes n}\otimes I_2\circ s\left(f_0\right)\circ H^{\otimes n}\otimes I_2\right]\circ s\left(f_a\right)\circ\left[H^{\otimes n}\otimes H\sigma_x\right]$$

and can be classically efficient simulated using classical computer. Where $a\in[0,N-1]$ is **P**'s chosen number, and moves (s_1) and (u_2) are repeated a total of $k=\left\lfloor\frac{\pi}{4}\sqrt{N}\right\rfloor$ times, i.e., $(s_k=\cdots=s_1)$ and$(u_k=\cdots=u_2)$. For $f:\mathbb{Z}_2^n\to\mathbb{Z}_2$, the oracle $s\left(f\right)$ is the permutation (and hence unitary transformation) defined by (see Table 3) $s\left(f\right)|x,b\rangle=|x,b\oplus f\left(x\right)\rangle$. Each **P**'s moves s_i can be thought of as the response of an oracle, which computes $f_x\left(x\right):=\delta_{xa}$ to respond to the quantum query defined by the state after the action of quantum strategy(u_i). After $O\left(\sqrt{N}\right)$ such queries, a measurement by $\Pi=|a\rangle\langle a|\otimes I_2$ returns a win for **Q** with probability bounded above$\frac{1}{2}$, i.e., Grover's QSA determines a with high probability [34].

Remark. If **Q** were to play classically, he could query **P** about a specific number at each time, but on the average it would take $\frac{N}{2}$ turns to guess$a$. A classical equilibrium is for **P** to choose a random, and for **Q** to choose a permutation of $N=2^n$ uniformly at random and guess numbers in the corresponding order. Even when **P** plays such a mixed strategy, **Q**'s quantum strategy is optimal; together they define mixed quantum equilibrium.

Knowing all this, **P** responds that he will be to play, but that **Q** should only get one guess, not $k=\left\lfloor\frac{\pi}{4}\sqrt{N}\right\rfloor$. **Q** protests that this is hardly fair, but he will play, as long as **P** tells how his guess is to the chosen number. P agrees, and they play. **Q** is in every step win.

In this case **Q** is used slightly improved Berstein-Vazirani algorithm (see in details Appendix): Guess x and answer a are vectors in $\mathbb{Z}_2^n$, so $x\cdot a$ depends on the cosine of the angle between these vectors. Thus is seems reasonable to define the oracle "*how close a guess is to the answer*" to be the oracle response$f_a\left(x\right)\mapsto g_a\left(x\right):=x\cdot a$. Then **Q** plays as follows:

$\|0\ldots0,0\rangle$	$\xrightarrow[H^{\otimes n}\otimes H\sigma_x]{Q}$	$\frac{1}{\sqrt{N}}\sum_{x00}^{n-1}\|x\rangle\otimes\frac{1}{\sqrt{2}}(\|0\rangle-\|1\rangle)$	$\Rightarrow$	(u_1)
	$\xrightarrow[s(g_a)]{P}$	$\frac{1}{\sqrt{N}}\sum_{x=0}^{n-1}(-1)^{x\cdot a}\|x\rangle\otimes\frac{1}{\sqrt{2}}(\|0\rangle-\|1\rangle)$	$\Rightarrow$	(s_1)
	$\xrightarrow[H^{\otimes n}\otimes I_2]{Q}$	$\|a\rangle\otimes\frac{1}{\sqrt{2}}(\|0\rangle-\|1\rangle)$	$\Rightarrow$	(u_2)

using the following (more simple) quantum game gate:

$$G = \left[H^{\otimes n} \otimes I_2\right] \circ g_a(x) \circ \left[H^{\otimes n} \otimes H\sigma_x\right].$$

For $\Pi = |a\rangle\langle a| \otimes I_2$ again, **Q** wins with probability 1, having queried **P** only once.

Remark. Oracle, which responds in the Berstein-Vazirani algorithm with $x \cdot a \ (mod\ 2)$, is a "sophisticated database" by comparison with Grover's oracle in QSA, which only responds that a guess is correct or incorrect. And finally, entanglement is not required in Berstein-Vazirani QA for quantum-over-classical improvement. It is remarkably the slightly improved version of the Berstein-Vazirani algorithm does not create entanglement at any time step, but still solves this oracle problem with fewer queries than is possible classically [31, 35].

Let us consider the application of entanglement-free quantum control algorithm for robust KB design of FC.

4. Quantum computing for design of robust wise control

Decomposition of optimization process in design of robust KB in intelligent control system are separated in two steps: (1) global optimization based on QGSA; and (2) learning process based on QNN for robust approximation of teaching signal from QGSA.

Figure 3 shows the main tools and interrelations between Soft, Quantum and Quantum Soft Computing for simulation, global optimization, quantum learning and the optimal design of robust KB in intelligent control systems.

The main problem of KB-optimization based on soft computing is consistent in the following: the design process can use only one solution space for global optimization. As an example, let us consider a design of KB for fixed class of stochastic excitations on control object. If the design process bases on many solution spaces with different statistical characteristics of stochastic excitations on control object then GA cannot find global solution for optimal KB. In this case for global optimization of KB QGSA is used. New optimization methods of intelligent control system structures (based on quantum soft computing) are required also a modification of simulation methods for quantum computing.

There can introduce a quantum computational speed-up without the use of entanglement. In this case, it is seen that no resource increases exponentially. Let us now consider briefly the structure of quantum control algorithm for design of robust KB-FC in intelligent control system.

We will study the problem of design the intelligent robust control from different KB that are received with soft computing technology but that are non-robust with the different changing of conditions in initial states of control object, external stochastic excitations, reference signals etc.

We can see from concrete example below that it is possible to design robust intelligent KB using superposition of non-robust KBs. In this case the quality of control based on a new KB is more effective than particular KBs. We say that in this case *wise robust* control is introduced. According to the definition of wise control it means: "*wise* $\equiv$ *intelligent* $\otimes$ *smart*". This situation is similar to Parrondo Paradox in quantum game. For design process of wise control in this case the entanglement is not used and it is different from Parrondo Paradox.

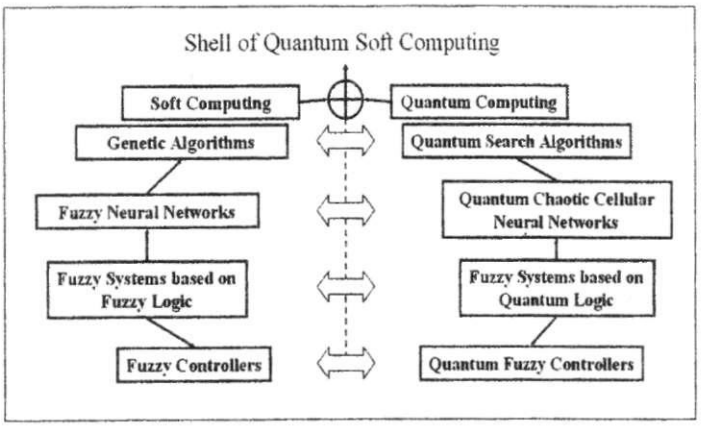


Figure 3: General structure of Quantum Soft Computing tools

Example: Entangled-free quantum control algorithm for design of robust wise KB-FC. Let us consider one of the examples of quantum computing approach to design robust wise quantum control. Figure 4a show the structure of intelligent control system based on fuzzy PD-controller (PD-FC). With Soft Computing optimizer we can design partial KB(i) for PD-FC from fuzzy simulation of control object behavior using different class of stochastic excitations. For many cases these KB(i) are not robust if we use another types of stochastic excitations on control object, changing initial states, or changing the type of reference signals.

The problem consists in design of unified robust KB-FC from any finite number KB(i) look-up tables created by Soft Computing Optimizer simulation of intelligent fuzzy control under fixed type stochastic excitations. Let us consider one of possible solution of this problem based on quantum computational algorithm. According to soft computing design technology of KB for FC we consider the ordered (structured) DB as control laws of coefficient gains in traditional controller as PID-controller. Superposition operator is used for design of relations between coefficient gains of PD-FC (see, Figure 4b).

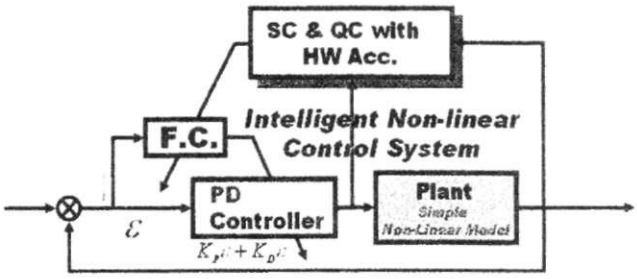


Figure 4a: Intelligent nonlinear control system

Grover's QSA is used for searching of solutions and max operation between decoding states is analogy of measurement process of solution search.

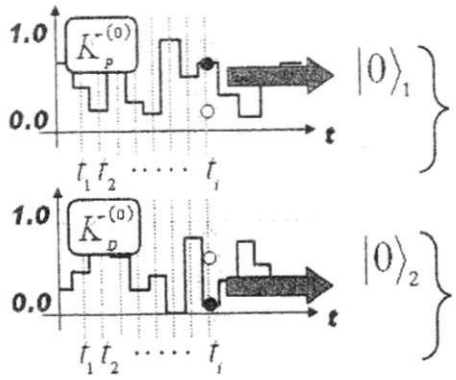


Figure 4b: Superposition of coefficient gains

Step	Computational algorithm
1	*Prepare two registers of* n *qubits in the state* $\|0\ldots0\rangle \in H_N$.
2	*Apply* H *over the first register*
3	*Apply diffusion (interference) operator* G *over the whole quantum state*
4	*Apply max operation over the first register*
5	*Measure the first register and output the measured value*

Figure 5 shows the structure of design process. As superposition operator we use the particular case of QFT - the Walsh-Hadamard transform.

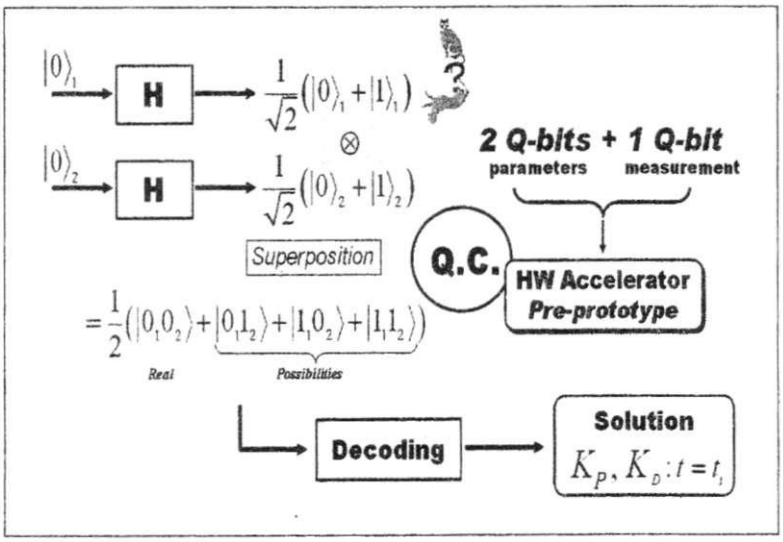


Figure 5: Structure of design process

$KB(i)$ of PD-FC includes the set of coefficient gains $K = \{k_P(t), k_D(t)\}$laws received from soft computing simulation using different types of random excitations on control object. Figure 6 show the structure of quantum control algorithm for design of a robust unified KB-FC from two KB-FC created by soft computing optimizer for Gaussian ($KB(1)$) and non-Gaussian (with Rayleigh probability density function) – $KB(2)$ noises.

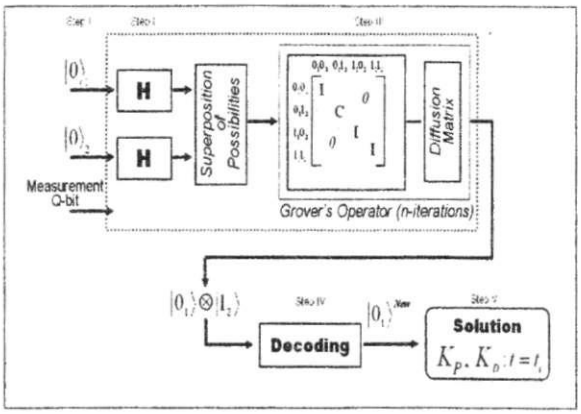


Figure 6: Robust KB design with quantum algorithm

Remark. From normalized real simulated coefficient gains $\{K_P(t), K_D(t)\}$can be calculated the values of virtual coefficient gains $\left\{k_P^Q(t), k_D^Q(t)\right\}$ as logical negation: $\left\{k_P^Q(t), k_D^Q(t)\right\} = 1 - \{k_P(t), k_D(t)\}$. For example, if the value of the proportional coefficient gain.$k_P(t_i)$, is $k_P(t_i) = 0,2$, then $k_P^Q(t_i) = 1 - 0,2 = 0.8$.

Figure 5 shows the geometrical interpretation of this computational process.

Figure 5 show the logical description of superposition between real and virtual values of coefficient gains created by soft computing simulation. For this case four classical states are joint in one non-classical superposition state with amplitude probability$\frac{1}{2}$. For above described example we have the following coding result:$|0_1\rangle \rightarrow 0.2$, $|1_1\rangle \rightarrow 0.8$.

Let us consider the computational steps of quantum control algorithm (see, Figure 6):

1	*Step 1 in quantum algorithm is the coding of current values (for fixed time t_i) of coefficient gains real values*
2	*According to the second step of algorithm Hadamard matrices are created superposition between real simulated and virtual classical states.* *Virtual classical state is calculated from normalized scale $[0,1]$ and according to complementary quantum law is logical negation of real simulated value.* *Remark. Hadamard transform joint two classical states in one non-classical state as superposition: $\frac{1}{\sqrt{2}}\left[|0_i\rangle + |1_i\rangle\right] = \frac{1}{\sqrt{2}}\left[|Yes\rangle + |No\rangle\right]$ that it is impossible in classical mechanics. This operation created the possibility for extraction of hidden quantum information from classical contradictory states.*
3	*In third step Grover's diffusion operator as interference operation search the solution*
4	*Max operation in step 4 is applied to classical states in superposition after decoding of results*
5	*Step 5 give the final results of quantum computation of new control laws of coefficient gains from two KB(i), i=1,2 created from soft computing technology*

Figure 7a shows the initial control laws of coefficient gains in PD-FC created from soft computing technology for essentially non-linear control object as *van der Pol* oscillator

$$\ddot{x} + \left(x^2 - 1\right)\dot{x} + x = k_P\left(t\right) e + k_D\left(t\right) \dot{e} + \xi\left(t\right) \tag{7}$$

under Gaussian random white noise $\xi\left(t\right)$.

Figure 7b shows the initial control laws of coefficient gains $\{k_P\left(t\right), k_D\left(t\right)\}$in PD-FC created from soft computing technology for similar essentially non-linear control object as Van der Pol oscillator under non-Gaussian random noise with Rayleigh probability distribution. Figure 7c shows the computational results of new coefficient gains of PD-FC based on the quantum control algorithm for similar essentially non-linear control object as Van der Pol oscillator using KB's created from soft computing technology. Figure 7d shows the results of simulation the dynamic behavior of Van der Pol oscillator using PD-FC with different KB.

The comparison of simulation results represented in Figure 7d shows the more robustness degree of quantum PD-FC than in similar classical soft computing cases as a new effect in intelligent control system design: From two non-robust KB of PD-FC's one robust KB of PD-FC with quantum computation approach can be design. This effect is similar to the effect in above mentioned quantum *Parrondo Paradox* in corresponding game but without using of entanglement.

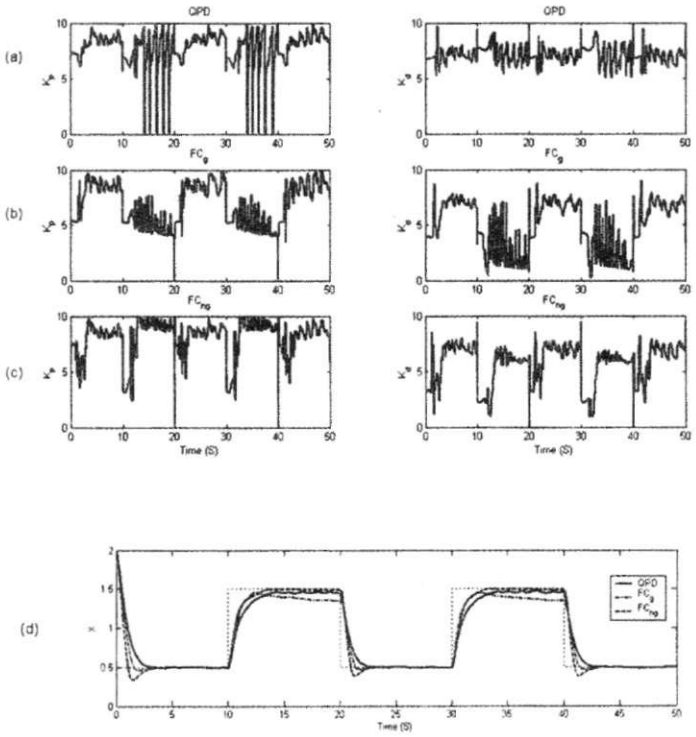


Figure 7: (a) Coefficient gains of Q-PD controller; (b) Coefficient gains scheduled by FC trained for Gaussian excitation; (c) Coefficient gains scheduled by FC trained for non-Gaussian excitation (d) Control object dynamics

5. Conclusions

We have developed new methods of quantum control process simulation with applications to AI, applied informatics and computer science. The QAG's design method on the examples as Grover's QSA and quantum games are illustrated. New effects of wise control design from non-robust KBs are described. The developed analysis and synthesis of QAG's dynamic are the background for silicon circuit gate design and simulation of robust knowledge base (KB) for intelligent fuzzy controllers (FC).

References

[1] Ulyanov S.V., Litvintseva L.V., Takahashi K. Computational intelligence with quantum game's approach and robust decision-making in communication information uncertainty // Proc. Intern. Conf. on Computational Intelligence (ICCI'2004). Nicosis. North Cyprus, 2004. P. 172 – 187.

[2] Kitaev A.Yu., Shen A.H. and Vyalyi M.N. Classical and quantum computation. Graduate Studies in Mathematics, Vol.47, American Mathematical Society (AMS), Providence, Rhode Island, 2002 (Translated from Russian Edition, 1999)

[3] Gruska J. Quantum computing. Advanced Topics in Computer Science Series, McGraw-Hill Companies, London, 1999

[4] Nielsen M.A., Chuang I.L. Quantum computation and quantum information. Cambridge University Press, Cambridge, England, 2000.

[5] Hirvensalo M. Quantum computing. Natural Computing Series, Springer-Verlag, Berlin, 2001.

[6] Hardy Y. and Steeb W.-H. Classical and quantum computing with C++ and Java Simulations. Birkhauser Verlag, Basel, 2001.

[7] Hirota O. The foundation of quantum information science: Approach to quantum computer (in Japanese). Japan, 2002

[8] Ulyanov S.V., Degli Antoni G., Yamafuji K., et all. Physical limits and information bounds of micro control. Part 2: Quantum soft computing and quantum searching algorithms // Proc. 1998 International Symposium on Micromechatronics and Human Science (MHS'98). Nagoya, Japan, 1998. P. 217 – 224.

[9] Petrov B.N., Ulyanov S.V., Goldenblat I.I. Control problems of relativistic and quantum dynamic objects: Information and thermodynamics approaches. Science Publ., Moscow, 1982.

[10] Ulyanov S.V., Kurawaki I., Yazenin A.V. Information analysis of quantum gates for simulation of quantum algorithms on classical computers // Proc. Quantum Communication, Computing and Measurements. Kluwer Academic / Plenum Publishers. V. 3. 2001. P. 207 – 214.

[11] Ghisi F. and Ulyanov S.V. Information role of entanglement and interference operators in Shor's quantum algorithm gate dynamics // J. Modern Optics. 2000. V. 47. No 12. P. 2079 – 2090.

[12] Ulyanov S.V., Rizzotto G.G., Kurawaki I. et all. Method and hardware architecture for controlling a process or for processing data based on quantum soft computing // PCT Patent WO 01/67186 A1, 2000.

[13] Ulyanov S.V., Ghisi F., Kurawaki I., Litvintseva L.V. Simulation of quantum algorithms on classical computers. Universita degli Studi di Milano, Polo Didattico e di Rcerca di Crema, Note del Polo. V. 32. 2000. 118 p.

[14] Ulyanov S.V. System and method for control using quantum soft computing // US patent No 6.578.018B1. 2003.

[15] Parrondo J.M.R., Harmer G.P., Abbott D. New paradoxical game based on Brownian ratchets // Phys. Rev. Lett. 2000. V. 85. No 24. P. 5226-5229.

[16] Flitney A.P., Ng J., Abbott D. Quantum Parrondo's games // Physica A. 2002. V. A314. No1. P. 35 – 42.

[17] D'Adriano G.M., Gill R.D., Keyl M. et all. The quantum Monty Hall problem // Quantum Information and Computation. 2002. V. 2. No 5. P. 355-366.

[18] Lee C.F., Johnson N.F. Exploiting randomness in quantum information processing // Phys. Lett. 2002. V. A301. No 6. P. 343-349.

[19] Lee C.F., Johnson N.F. Parrondo games and quantum algorithms // arXiv: quant-ph/ 0203043 v1 10 Mar 2002. 7p.

[20] Marinatto L., Weber T. A quantum approach to static games of complete information // Phys. Lett. 2000. V. A272. No 6. P. 291-303.

[21] Du J., Xu X., Li H. et all. Entanglement playing a dominant role in a quantum games // Phys. Lett. 2001. V. A289. No 1. P. 9-15.

[22] Du J., Xu X., Li H. et all Entanglement enhanced multiplayer quantum games // Phys. Lett. 2002. V. A302. No 6. P. 229-233.

[23] Flitney A.P., Abbott D. Miracle moves in 2×2 quantum games // arXiv: quant-ph/0209121 24 Sep2002, 10p.

[24] Iqdal A., Toor A.H. Entanglement and dynamic stability of Nash equilibria in a symmetric quantum game // Phys. Lett., 2001, V. A286, No 4. P. 245-250.

[25] Peres A., Wootters W.K. Optimal detection of quantum information // Phys. Rev. Lett. 1991. V. 66. No 9. P. 1119-1122.

[26] Chou C.-L., Hsu L.Y. Optimal guessing strategies in a quantum card game // arXiv: quant-ph/0206167 v1 24 Jun 2003. 11p.

[27] Orùs R., Lattore J.I., Martin-Delgado M.A. Systematic analysis of majorization in quantum algorithms // arXiv: quant-ph/0212094v1 16 Dec 2002. 13p.

[28] Meyer D.A. Quantum strategies // Phys. Rev. Lett.1999. V. 82. No 5. P.1052 - 1055.

[29] Du J., Xu X., Li H. et all. Quantum strategy without entanglement // arXiv: quant-ph/0011078 19Nov 2000. 4p.

[30] Meyer D.A. Sophisticated quantum search without entanglement // Phys. Rev. Lett. 2000. V. 85. No 9. P. 2014-2016.

[31] Meyer D.A. Quantum games and quantum algorithms // AMS Contemporary Mathematics Volume: Quantum Computation and Quantum Information Science. 2000. (available in **arXiv**: quant-ph/0004092 24 Apr 2000. 10p.)

[32] Kashefi E., Kent A., Vedral V. et all. Comparison of quantum oracles // Phys. Rev. 2002. V. 65 A. No 5. P. 050304-1-050304-4.

[33] Kim J., Lee S., Chi D.P. Quantum functional oracles // J. Phys. A. 2002. V. 35. No12. P. 6911-6917.

[34] Boyer M., Brassard G., Hoyer P., Tapp A. Tight bounds in quantum searching // Fortschr. Phys.1998. V. 46, No 4/5. P. 493-505.

[35] Maucrer S., Hogg T., Huberman B.A. Portfolios of quantum algorithms // Phys. Rev. Lett. 2001. V. 87, No 25. P. 257901.

[36] Arikan E. An information-theoretic analysis of Grover's algorithm // arXiv: quant-ph/0210068 10 Oct 2002. 9p.

Appendix. Grover's quantum search algorithm: Information analysis of quantum gate dynamics.

Quantum algorithms come in two main varieties: the ones that rely on a Fourier transform, and the ones that rely on amplitude amplification. Typically the algorithms consist of a sequence of trials. After each trial a measurement of the system produces a desired state with some probability determined by the amplitudes of the superposition created by the trial. Trials continue until the measurement gives a solution, so that the number of trials and hence the running time are random variable. Let us consider the same problems for concrete Grover's QSA based on amplitude amplification.

A.1. Dynamics of Grover's QSA gate. Grover's algorithm starts by preparing all m qubits of the quantum computer in the state$|s\rangle = |0\ldots0\rangle$. An elementary rotation in the direction of the sought state $|x_0\rangle$ with property $f(x_0) = 1$ is achieved by the gate sequence:

$$Q = -\left[\underbrace{\left(I_s H^{\otimes 2m}\right)\cdot I_{x_0}}_{k\ times}\right]\cdot H^{\otimes 2m}, \quad \text{(A.1)}$$

where the phase inversion I_s with respect to the initial state $|s\rangle$ is defined by $I_s|s\rangle = -|s\rangle$, $I_s|s\rangle = |s\rangle$ $(x \neq s)$. The controlled phase inversion I_{x_0} with respect to the sought state $|x_0\rangle$ is defined in an analogous way. Because the state $|x_0\rangle$ is not known explicitly but only implicitly through the property$f(x_0) = 1$, this transformation has to be performed with the help of the quantum oracle. This task can be achieved by preparing the ancillary of the quantum oracle in the state $|a_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ as the unitary and Hermitian transformation$U_F : |x, a\rangle \rightarrow |x, f(x) \oplus a\rangle$. Thereby$|x\rangle$ is an arbitrary element of the computational basis and $|a\rangle$ is the state of an additional ancillary qubit. As a consequence one obtains the required properties for the phase inversionI_{x_0}, namely [4]:

$$|x, f(x) \oplus a_0\rangle \equiv |x, 0 \oplus a_0\rangle \quad = \quad \frac{1}{\sqrt{2}}[|x,0\rangle - |x,1\rangle] = |x, a_0\rangle, \quad for\ x \neq x_0$$

$$|x, f(x) \oplus a_0\rangle \equiv |x, 1 \oplus a_0\rangle \quad = \quad \frac{1}{\sqrt{2}}[|x,1\rangle - |x,0\rangle] = -|x, a_0\rangle, \quad for\ x = x_0$$

In order to rotate the initial state $|s\rangle$ into the state $|x_0\rangle$ one has to perform a sequence of n such rotations and a final Hadamard transformation at the end, i.e., $|s_{fin}\rangle = HQ^n |s_{in}\rangle$. The optimal number n of repetitions of the gate Q in Eq. (A.1) is approximately given by

$$n = \frac{\pi}{4\arcsin\left(2^{-\frac{m}{2}}\right)} - \frac{1}{2} \approx \frac{\pi}{4}\sqrt{2^m}, \ (2^m \gg 1). \ (A.2)$$

The Grover's algorithm is optimal [4 - 6].

A.2. Quantum operators of QSA. The distinctive element of this algorithm isD_n, which is called *diffusion matrix* [35] of order $n$and it is responsible of interference in this algorithm.

Table A1: Diffusion matrix definition

D_n	|0..0>	|0..1>	...	|i>	...	|1..0>	|1..1>
|0..0>	$-1+1/2^{n-1}$	$1/2^{n-1}$	...	$1/2^{n-1}$	...	$1/2^{n-1}$	$1/2^{n-1}$
|0..1>	$1/2^{n-1}$	$-1+1/2^{n-1}$	...	$1/2^{n-1}$	...	$1/2^{n-1}$	$1/2^{n-1}$
...	...	...	...	...	...	...	...
|i>	$1/2^{n-1}$	$1/2^{n-1}$	...	$-1+1/2^{n-1}$	...	$1/2^{n-1}$	$1/2^{n-1}$
...	...	...	...	...	...	...	...
|1..0>	$1/2^{n-1}$	$1/2^{n-1}$	...	$1/2^{n-1}$	...	$-1+1/2^{n-1}$	$1/2^{n-1}$
|1..1>	$1/2^{n-1}$	$1/2^{n-1}$	...	$1/2^{n-1}$	...	$1/2^{n-1}$	$-1+1/2^{n-1}$

It plays the same role as QFT_n (*Quantum Fourier Transform*) in Shor's algorithm and of ${}^nH$ in Deutsch-Jozsa's and Simon's algorithms.

This matrix is defined as

$$[D_n]_{i,j} = \frac{(-1)^{i\,AND(i=j)}}{2^{n/2}}, \ (A.3)$$

where $i = 0, ..., 2^n - 1$, $j = 0, ..., 2^n - 1$ n is a number of inputs.

The gate equation of Grover's QSA circuit is the following:

$$G^{Grover} = [(D_n \otimes I) \cdot U_F]^h \cdot ({}^{n+1}H) \ (A.4)$$

Example. The diagonal matrix elements in Grover's QSA-operators (as example Eq. (A.5)) are connected a database state to itself and the off-diagonal matrix elements are connected a database state to its neighbours in the database. The diagonal elements of the diffusion matrix have the opposite sign from the off-diagonal elements. The magnitudes of the off-diagonal elements are roughly equal, so we can write the action of the matrix on the initial state, as example:

$$\begin{pmatrix} -a & b & b & b & b & b \\ b & -a & b & b & b & b \\ b & b & -a & b & b & b \\ b & b & b & -a & b & b \\ b & b & b & b & -a & b \\ b & b & b & b & b & -a \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ -1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \frac{1}{\sqrt{N}} = \begin{pmatrix} -a+(N-3)b \\ -a+(N-3)b \\ +a+(N-1)b \\ -a+(N-3)b \\ -a+(N-3)b \\ -a+(N-3)b \end{pmatrix} \frac{1}{\sqrt{N}}, \ (A.5)$$

where $a = 1-b$, $b = \frac{1}{2^{n-1}}$. If one of the states is marked, i.e. has its phase reserved with respect to those of the others, the multimode interference conditions are appropriate the constructive interference to the marked state, and destructive interference to the others. That is, the population in the marked bit is amplified. The form of this matrix is identical to that obtained through the inversion about the average procedure in Grover's QSA. This operator produce a contrast in the probability density of the final

states of the database of $\frac{1}{N}\left[a+(N-1)b\right]^2$ for marked bit versus $\frac{1}{N}\left[a-(N-3)b\right]^2$ for the unmarked bits; N is the number of bits in the data register. Grover algorithm gate in Eq. (A.1) is optimal and it is very efficient search algorithm. And Grover-based software is currently used for search routines in large database [2 - 7].

A.3. Information analysis and optimization of QSA-termination problem. Grover's QSA consists of a number of trials repeated until a solution is found. Each trial has a predetermined number of iterations, which determines the probability of finding a solution. It is therefore necessary to carefully choose their number to optimize the running time. These problems are studied in [11, 34]. A quantitative measure of success in the database search problem is the reduction of the information entropy of the system following the search algorithm [14]. Entropy $S^{Sh}(P_i)$ in this example of a single marked state is defined as

$$S^{Sh}(P_i) = -\sum_{i=1}^{N} P_i \log P_i, \quad \text{(A.6)}$$

where P_i is the probability that the marked bit resides in orbital i. In general, according to [9], the von Neumann entropy is not a good measure for the usefulness of Grover's algorithm. For practically every value of entropy, there exit states are good initializers and states that are not. For example,$S\left(\rho_{(n-1)-mix}\right) = \log_2 N - 1 = S\left(\rho_{\left(\frac{1}{\log_2 N}\right)-pure}\right)$, but when initialized in $\rho_{(n-1)-mix}$, the Grover algorithm is as bad as guessing the market state. Another example may be given using pure states $H|0\rangle\langle 0|H$ and$H|1\rangle\langle 1|H$. With the first, Grover arrives to the marked state quadratic speed-up, while the second is practically unchanged by the algorithm. We used the Shannon information entropy for optimization of the termination problem of Grover's QSA [14]. Information analysis of Grover's QSA based on using of Eq. (A.6), gives a lower bound on necessary amount of entanglement for searching of success result and of computational time: any QSA that uses the quantum oracle calls $\{O_s\}$ as $I-2|s\rangle\langle s|$ must call the oracle at least $T \geqslant \left(\frac{1-P_e}{2\pi}+\frac{1}{\pi \log N}\right)\sqrt{N}$ times to achieve a probability of errorP_e [36].

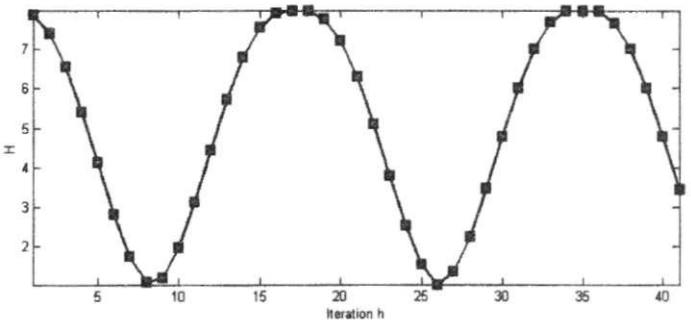


Figure A1: Shannon entropy analysis of Grover's QSA dynamics with seven inputs

The information system consists of the N-state data register. Physically, when the data register is loaded, the information is encoded as the phase of each orbital. The orbital amplitudes carry no information. While state-selective measurement gives as result only amplitudes, the information is completely hidden from view, and therefore the entropy of the system is maximum:$S^{Sh}_{init}(P_i) = -\log(1/N) = \log N$. The rules of

quantum measurement ensure that only one state will be detected each time. If the algorithm works perfectly, the marked state orbital is revealed with unit efficiently, and the entropy drops to zero.

Otherwise, unmarked orbital may occasionally be detected by mistake. The entropy reduction can be calculated from the probability distribution, using Eq. (A.6). Figure A1 show the result of entropy calculation for the simulation quantum search of one marked state in the case $N = 7$. The minimum Shannon entropy criteria is used for successful termination of Grover's QSA and realized in this case in digital circuit implementation. Experimental success results of Grover's QSA simulation with information condition of QSA-termination are demonstrated in [12, 14].