

INFORMATION DYNAMIC ANALYSIS AND MEASURE OF QUANTUM ALGORITHM'S COMPUTATIONAL INTELLIGENCE

Barchatova Irina¹, Degli Antonio Giovanni², Ulyanov Sergey³

¹PhD Student;

Dubna International University of Nature, Society and Man,
Institute of system analysis and management;
141980, Dubna, Moscow reg., Universitetskaya str., 19;
e-mail: i.a.barhatova@gmail.com.

²PhD, professor;

Polo Didattico e di Ricerca di Crema;
Via Bramante, 65-26013, Crema (CR), Italy;
e-mail: gda@dsi.unimi.it.

³Doctor of Science in Physics and Mathematics, professor;

Dubna International University of Nature, Society and Man,
Institute of system analysis and management;
141980, Dubna, Moscow reg., Universitetskaya str., 19;
e-mail: ulyanovsv@mail.ru.

Information dynamic analysis of main quantum algorithms is described. The qualitative analysis of quantum information is introduced. Measure of quantum algorithm's computational intelligence is discussed.

Keywords: Information analysis, information measure of quantum algorithm's computational intelligence, qualitative analysis of efficiency simulations.

ИНФОРМАЦИОННЫЙ ДИНАМИЧЕСКИЙ АНАЛИЗ И МЕРЫ ИНТЕЛЛЕКТУАЛЬНОСТИ КВАНТОВЫХ АЛГОРИТМОВ

Бархатова Ирина Александровна¹, Джiovанни дели Антонио², Ульянов Сергей Викторович³

¹Аспирант;

ГБОУ ВО «Международный Университет природы, общества и человека «Дубна»,
Институт системного анализа и управления;
141980, Московская обл., г. Дубна, ул. Университетская, 19;
e-mail: i.a.barhatova@gmail.com.

²Доктор наук, профессор;

Поло дидаттико, Крема, факультет информационных технологий;
Италия, Крема, Виа Браманте, 65-26013;
e-mail: gda@dsi.unimi.it.

³Доктор физико-математических наук, профессор;

ГБОУ ВО «Международный Университет природы, общества и человека «Дубна»,
Институт системного анализа и управления;
141980, Московская обл., г. Дубна, ул. Университетская, 19;
e-mail: ulyanovsv@mail.ru.

Представлен информационный анализ основных квантовых алгоритмов и качественный анализ квантовой информации. Рассмотрены меры вычислительного интеллекта квантовых алгоритмов.

Ключевые слова: информационный анализ, информационное измерение интеллектуальности квантовых алгоритмов, качественный анализ эффективности моделирования.

Introduction: Information analysis axioms of quantum algorithm dynamic evolution

The qualitative analysis of quantum information is described in [1 – 5]. Any computation (both classical and quantum) is formally identical to a communication in time. By considering quantum computation as a communication process, it is possible to relate its efficiency to its classical communication capacity. At time $t = 0$, the programmer (\underline{M}) sets the computer to accomplish any one of several possible tasks. Each of these tasks can be regarded as embodying a different message. Another programmer (\underline{C}) can obtain this message by looking at the output of the computer when the computation is finished at time $t = T$. Computation based on quantum principles allows for more efficient algorithms for solving certain problems than algorithms based on pure classical principles.

Remark 1. The sender conveys the maximum information when all the message states have equal *a priori* probability (which also maximizes the channel capacity). In that case the mutual information (channel capacity) at the end of the computation is $\log N$.

The communication capacity gives an index of efficiency of a quantum computation [6]:

A necessary target of a quantum computation is to achieve the maximum possible communication capacity consistent with given initial states of the quantum computing.

Let us consider any peculiarities of information axioms and information capability of quantum computing as the dynamic evolution of quantum algorithms (QAs). If one breaks down the general unitary transformation U_i of a QA into a number of successive unitary blocks, then the maximum capacity may be achieved only after the number of applications of the blocks. In each of the smaller unitary blocks, the mutual information between the \underline{M} and the \underline{C} registers (i.e., the communication capacity) increases by a certain amount. When its total value reaches the maximum possible value consistent with a given initial state of the quantum computing, the computation is regarded as being complete (see, in details [6, 7]). The classical capacity of a quantum communication channel is connected with the efficiency of quantum computing using *entropic* arguments. This formalism allows us to derive lower bounds on the computational complexity of QA's in the most general context. The following qualitative axiomatic descriptions of dynamic evolution of information flow in a QA are provided [8, 9]:

N	Axiomatic Rules
1	The information amount (information content) of a successful result increases while the QA is in execution
2	The quantity of information becomes the fitness function for the recognition of successful results on intelligent states and introduces the measures of accuracy and reliability (robustness) for successful results.
	In this case the principle of Minimum of Classical / Quantum Entropy (MCQE) corresponds to recognition of successful results on intelligent states of the QA computation
3	If the classical entropy of the output vector is small, then the degree of order for this output state relatively larger, and the output of measurement process on intelligent states of a QA gives the necessary information to solve the initial problem with success

Remark 2. These three information axioms mean that the algorithm can automatically guarantee convergence of information amount to a desired precision with a minimum decision making risk. This is used to provide robust and stable results for fault-tolerant quantum computation. Main information measures in classical and quantum domains are shown in Tables 1 and 2.

Table 1. Typical measures of information amount

Title	Classical(CI)	Quantum(Q)
<i>Fisher</i>	$F^{Cl}(x) = \int \frac{1}{p(\xi x)} \left(\frac{\partial p(\xi x)}{\partial x} \right)^2 d\xi$	$F^Q(x) = \int \frac{Tr \left[\left(\hat{E}(\xi) \frac{\partial \rho(x)}{\partial x} \right) \right]^2}{Tr(\hat{E}(\xi)\rho(x))} d\xi$
<i>Boltzman – Shannon</i> ↓ <i>von Neumann</i>	$S^{Sh} = -\sum_i p_i \ln p_i$	$S^{vN} = -Tr(\rho \ln \rho)$
<i>Relative Information – Kullback – Leibler</i>	$I^{Cl}(p:q) = -\sum_i p_i \ln \frac{q_i}{p_i}$	$I^Q(\rho:\sigma) = -Tr\left(\rho \ln \frac{\rho}{\sigma}\right)$
<i>Renyi</i>	$S_q^{(Cl)R} = \frac{1}{1-q} \ln \left(\sum_{i=1}^W p_i^q \right)$	$S_q^{(Q)R} = \frac{\ln [Tr(\rho^q)]}{1-q}$
<i>Havrda & Charvat – Daróczy (Tsallis)</i>	$S_q^{(Cl)T} = \frac{\left(1 - \sum_{i=1}^W p_i^q \right)}{1-q}$	$S_q^{(Q)T} = \frac{(1 - Tr(\rho^q))}{1-q}$

Table 2. Relations between different typical measures of information amounts

1. <i>Shannon and von Neumann Entropy Relation</i> $S^{vN} \leq S^{Sh}$ For Diagonal Density Matrix: $\rho = \rho_{ii}$ and $S^{vN} = S^{Sh}$
2. <i>Tsallis q-Entropy and Shannon Entropy Relation</i> $\lim_{q \rightarrow 1} S_q^{(Cl)T} = \lim_{q \rightarrow 1} S_q^{(Cl)R} = -\sum_{i=1}^W p_i \ln p_i$
3. <i>Tsallis q-Entropy and Renyi Entropy Relation</i> $S_q^{(Cl)R} = \frac{\ln [1 + (1-q) S_q^{(Cl)T}]}{1-q}$

Remark 3. Five main information-based approaches in optimal design of QA's computation can be used: 1) the maximum entropy (ME) principle; 2) minimum Fisher information (MFI) principle; 3) principle of extreme physical information (EPI); 4) principle of maximum of mutual information (MMI) between computational and measurement dynamic evolution (computational and memory registers) of QA's; and 5) principle of maximal intelligence of QA's based on minimum of difference between classical and quantum entropies in intelligent states of successful results. The first three principles (ME, MFI, and EPI) are based on the physical laws and may be derived through variation on appropriate Lagrangian's and includes in last two principles according to relations between the classical and quantum entropies, and mutual information amount.

The main properties of quantum information and entropy measures, and interrelations between information amounts (classical and quantum measures) are described in [8].

Remark 5. The EPI principle differs significantly from the EM approach or the MFI approach: (1) In its aims (establishing on ontology in EPI and eliciting the laws of physics from a consideration of the flow of information in the measurement process, vs subjectively estimating the laws in ME or MFI); (2) in its reason for extremization (conservation of information in EPI, vs arbitrary, subjective and sometimes inappropriate choice of «maximum smoothness» in ME and MFI); (3) how «constraints» are chosen (via the invariance of information to a symmetry operation principle in EPI vs arbitrary subjective choice in ME or MFI); and (4)

in its solutions (to a differential equation in EPI and MFI, vs a solution, always in the form of an exponential of a function, in ME). Only *EPI* applies broadly to all of physics principles^{1,2,3,4,5}.

Information intelligent measure of QA's (principle 5)

The information intelligent measure of QA as $I_T(|\psi\rangle)$ of the state $|\psi\rangle$ with respect to the qubits in T and to the basis $B = \{|i_1\rangle \otimes \dots \otimes |i_n\rangle\}$ is [8, 9]

$$\mathcal{I}_T(|\psi\rangle) = 1 - \frac{S_T^{Sh}(|\psi\rangle) - S_T^{VN}(|\psi\rangle)}{|T|} \quad (0)$$

The measure (0) is minimal (i.e., 0) when $S_T^{Sh}(|\psi\rangle) = |T|$ and $S_T^{VN}(|\psi\rangle) = 0$, it is maximal (i.e., 1) when $S_T^{Sh}(|\psi\rangle) = S_T^{VN}(|\psi\rangle)$.

The intelligence of the QA state is maximal if the gap between the Shannon and the von Neumann entropy for the chosen result qubit is minimal. Information QA-intelligent measure (0) and interrelations between information measures in Table 2 are used together with the step-by-step natural majorization principle for solution of QA-stopping problem. Due to the presence of quantum entropy, QA cannot obviate Bellman's «*the curse of dimensionality*» encountered in solving many complex numerical and optimization problems. And finally, the stringent condition that quantum computers have to be interaction-free, leave them with little versatility and practical utility. It has been seen that large entanglement of the quantum register is a necessary condition for exponential speed-up in quantum computation. It is one of reasons to why the quantum paradigm is not so easy to extend to all the classical computational algorithms and also explain the failure of programmability and scalability in quantum speed-up.

Remark 6. To be concrete, a quantum register such that the maximum Schmidt number (see below) of any bipartition is bounded at most by a polynomial in the size of the system can be simulated efficiently by classical means. The universality study of scaling of entanglement in Shor's factoring algorithm and in adiabatic QAs across a quantum phase transition for both the NP-complete Exact Cover problem (as a particular case of the 3-SAT problem) as well as the Grover's problem shows as following: (i) analytical result for Shor's QA's is a linear scaling of the entropy in terms of the number of qubits, therefore difficult the possibility of an efficient classical simulation protocol; (ii) a similar result is obtained numerically for the quantum adiabatic evolution Exact Cover algorithm, which also universality of the quantum phase transition the system evolves nearby; and (iii) entanglement in Grover's adiabatic QSA remains a bounded quantity even at the critical point. For these cases a classification of scaling of entanglement appears as a natural grading of the computational complexity of simulating quantum phase transitions.

Information analysis and computational intelligence measures of the quantum decision making algorithm

Most of the applications of quantum information theory have been developed in the domain of quantum communications systems, in particular in quantum source coding, quantum data compressing and quantum error-correcting codes. In parallel, QA's have been studied as computational processes, concentrating attention on their dynamics and ignoring the information aspects involved in quantum computation. In the follow-

¹ Syska J. Frieden wave function representations via an EPR-Bohm experiment // arXiv:1309.6957v1 [quant-ph] 17 Jul 2013.

² Liou Ch.-Y., Peng J.-Y. Physical phenomenon from the viewpoint of information (Introduction to quantum information theory) // <http://red.csie.ntu.edu.tw/publications/information.pdf> March 28, 2004.

³ Flego S.P., Plastino A., Plastino A.R. Fisher information and quantum mechanics // Intern. Research J. of Pure and Appl. Chemistry. – 2012. – Vol. 2. – № 1. – Pp. 25-54.

⁴ Востовский Г.В. Элементы информационной физики. – М.: МГИУ. – 2002. – С. 260.

⁵ Frieden, B.R. Science from Fisher information measure. – Cambridge: Cambridge University Press. – 2004.

ing section, the application of tools and techniques from quantum information theory in the domain QA's synthesis and simulation is described. For this purpose, the analysis of the classical and quantum information flow in Deutsch-Jozsa algorithm is used. It is shown that the quantum algorithmic gate (QAG) G , based on superposition of states, quantum entanglement and interference, when acting on the input vector, stores information into the system state, minimizing the gap between classical Shannon entropy and quantum von Neumann entropy.

This principle is fairly general, resulting in both a methodology to design a QAG and a technique to simulate (efficiently) its behavior on a classical computer.

The following disclosure uses classical and quantum correlations to describe QA computation. Classical correlations play a more prominent role than quantum correlations in the speed-up of certain QAs.

Information analysis of Deutsch algorithm

The advantage of quantum computing lies in the exploitation of the phenomenon of superposition. The great importance of the quantum theory of computation lies in the fact that it reveals the fundamental connections between the laws of physics and the nature of computation [7, 10, 11]. There is a great simplification in understanding quantum computation: a quantum computer is formally equivalent to a multi-particle *Mach-Zender*-like interferometer. Deutsch's QA is a simple example that illustrates the advantages of quantum computation.

Deutsch's QA as discussed in Chapter 1 is based on the assumption that a binary function of a binary variable $f: \{0,1\} \rightarrow \{0,1\}$ is given. Thus, $f(0)$ can be either 0 or 1, and $f(1)$ likewise can be either 0 or 1, giving altogether four possibilities. The problem posed by Deutsch's QA is to determine whether the function is constant [i.e., $f(0) = f(1)$], or varying [i.e., $f(0) \neq f(1)$].

Deutsch poses the following task: by computing f only once, determine whether it is constant or balanced. This kind of problem is generally referred to as a promise algorithm, because one property out of a certain number of properties is initially promised to hold, and the task is to determine computationally which one holds.

Classically, finding out in one step whether a function is constant or balanced is clearly impossible. One would need to compute $f(0)$ and then compute $f(1)$ in order to compare them. There is no way out of this double evaluation. Quantum mechanically, however, there is a simple method for performing this task by computing f only once. Two qubits are needed for the computation. In reality only one qubit is really needed, but the second qubit is there to implement the necessary transformation. Imagine that the first qubit is the input to the quantum computing whose internal Hardware (HW) part is represented by the second qubit.

The computational process itself will implement the following transformation on the two qubits (this is performed quantum mechanically, i.e., not using «classical» devices such as beam-splitters): $|x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$, where x is the input and y is the HW. Note that this transformation is reversible and thus there is a unitary transformation to implement it (in the basic principle). The function f has been used only once. The trick is to prepare the input in such a state to make use of quantum superposition.

The solution begins with the input $|x\rangle|y\rangle = (|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$, where $|x\rangle$ is the actual input and $|y\rangle$ is part of the computing HW. Thus, before the transformation is implemented, the state of the computing is an equal superposition of all four basis states, which are obtained by simply expanding the state $|x\rangle|y\rangle$ as

$$|x\rangle|y\rangle = |\psi_{in}\rangle = |00\rangle - |01\rangle + |10\rangle - |11\rangle.$$

Note that there are negative phase factors before the second and fourth terms.

When this state now undergoes the transformation in the abovementioned way $|x\rangle|y\rangle \rightarrow |x\rangle|y \oplus f(x)\rangle$, following output state is produced:

$$\begin{aligned} |\psi_{out}\rangle &= |0f(0)\rangle - |0\bar{f}(0)\rangle + |1f(1)\rangle - |1\bar{f}(1)\rangle \\ &= |0\rangle[|f(0)\rangle - |\bar{f}(0)\rangle] + |1\rangle[|f(1)\rangle - |\bar{f}(1)\rangle], \end{aligned}$$

where the over-bar indicates the opposite of that value, so that, for example, $\bar{0} = 1$.

The power of quantum computing is realized in that each of the components in the superposition of $|\psi_{in}\rangle$ underwent the same evolution «simultaneously» leading to the powerful «quantum parallelism». This feature is true for quantum computation in general. The possibilities are:

(1)	<i>If f is constant then</i>
$ \psi_{out}\rangle =$	$(0\rangle + 1\rangle)[f(0)\rangle - \bar{f}(0)\rangle]$
(2)	<i>if f is balanced then</i>
$ \psi_{out}\rangle =$	$(0\rangle - 1\rangle)[f(0)\rangle - \bar{f}(0)\rangle]$

Note that the output qubit (in this case the first qubit) emerges in two different orthogonal states, depending on the type of function f . These two states can be distinguished with probability 1 of efficiency. A Hadamard transformation performed on this qubit leads to the state $|0\rangle$ if the function is constant and to the state $|1\rangle$ if the state function is balanced. Now a single projective measurement in $\{|0\rangle, |1\rangle\}$ basis determines the type of the function.

Therefore, unlike their classical counterparts, quantum computing can solve Deutsch's problem. The input could also be of the form $(|0\rangle - |1\rangle)(|0\rangle - |1\rangle) \equiv |-\rangle|-\rangle$. A constant function would then lead to the state $|-\rangle|-\rangle$ and a balanced function would lead to $|+\rangle|-\rangle$. So the $|+\rangle$ and $|-\rangle$ are equally good as input states of the first qubit and both lead to quantum speed-up. Their equal mixture, on the other hand, is not. This means that the output would be an equal mixture $\frac{1}{2}(|+\rangle\langle+| + |-\rangle\langle-|)$ no matter whether $f(0) = f(1)$ or $f(0) \neq f(1)$, i.e., the two possibilities would be indistinguishable.

Thus for the QA to work well, one needs the first register to be highly correlated to the two different types of functions. If the output state of the first qubit is ρ_1 then function is balanced. The efficiency of Deutsch's algorithm depends on distinguishing the two states ρ_1 and ρ_2 . This is given by the Holevo bound,

$I_{acc} = S(\rho) - \frac{1}{2}[S(\rho_1) + S(\rho_2)]$, where $\rho = \frac{1}{2}(\rho_1 + \rho_2)$. Therefore, if $\rho_1 = \rho_2$, then $I_{acc} = 0$ and the QA has no speed-up over the classical one. At the other extreme, if ρ_1 and ρ_2 are pure and orthogonal, then $I_{acc} = 1$ and the computation gives the right result in one step. In between these two extremes lie all other computations with varying degrees of efficiency as quantified by the Holevo-bound. These are purely classical correlations and there is no entanglement between the first and the second qubit. In fact, the Holevo-bound is the same as the formula for classical correlations. The key to understanding the efficiency of Deutsch's algorithm is, therefore, through the mixedness of the first register. If the initial state has the entropy of S_0 , then the final Holevo-bound is $\Delta S = S(\rho) - S_0$.

So, the more mixed the first qubit, the less efficient the computation. Note that the quantum mutual information between the first qubits is zero throughout the entire computation (so there are neither classical nor quantum correlations between them).

Information analysis of QAG dynamics and intelligent output states: Deutsch-Jozsa algorithm

Deutsch-Jozsa algorithm's dynamics of quantum computation states are analyzed from classical and quantum information theory standpoint. Shannon entropy is interpreted as the degree of information accessi-

bility through the measurement, and von Neumann entropy is employed to measure quantum correlation information of entanglement. A maximally intelligent state is defined as a QA successful computation output state with minimum gap between classical and quantum entropy. The Walsh-Hadamard transform creates maximally intelligent states for Deutsch-Jozsa's problem, since it annihilates the qubit gap between classical and quantum entropy for every state.

Computation dynamics of Deutsch-Jozsa QAG. In the Deutsch-Jozsa algorithm, an integer number $n > 0$ and a truth-function $f : \{0,1\}^n \rightarrow \{0,1\}$ are given such that f is either constant or balanced (where f is constant if it computes the same output for every input, it is balanced if it takes values 0 and 1 on 2^{n-1} input strings each.)

The problem is to decide whether f is constant or balanced.

Function f is encoded into a unitary operator U_F corresponding to a squared matrix of order 2^{n+1} , where $F : \{0,1\}^n \times \{0,1\} \rightarrow \{0,1\}^n \times \{0,1\}$ is an injective function such that:

$$F(x, y) = (x, y \oplus f(x)) \quad (1)$$

(\oplus is the XOR operator) and U_F is such that:

$$[U_F]_{i,j} = \delta_{i, 1 + [F([j-1])_{(2)}]_{(10)}} \quad (2)$$

($[r](b)$ is the basis b representation of number r , $\delta_{i,j}$ is the Kronecker delta); H denotes the unitary Walsh-Hadamard transform $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and nH the n -power of matrix H through tensor product. Operator U_F is embedded into a more general unitary operator called quantum algorithmic gate (QAG) as G

$$G = ({}^nH \otimes I) \cdot U_F \cdot {}^{n+1}H \quad (3)$$

(I denotes the identity matrix of order 2), which is applied to the input vector of dimension 2^{n+1} . In this context, ${}^{n+1}H$ plays the role of the superposition operator (*Sup*), U_F stands for the entanglement operator (*Ent*) and finally ${}^nH \otimes I$ is the interference operator (*Int*). The corresponding computation is described by the following steps:

Step	Computation Algorithm	Formula
Step0	$ input\rangle = 0\rangle \otimes 0\rangle \otimes \dots \otimes 0\rangle \otimes 1\rangle$	4(a)
Step1	$ \psi_1\rangle = H_{n+1} input\rangle = \frac{1}{\sqrt{2^n}} \sum_{i_1, \dots, i_n} i_1 \dots i_n\rangle \otimes \frac{(0\rangle - 1\rangle)}{\sqrt{2}}$	4(b)
Step2	$ \psi_2\rangle = U_F \psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{i_1, \dots, i_n} \left(-1^{f(i_1, \dots, i_n)} \right) i_1 \dots i_n\rangle \otimes \frac{(0\rangle - 1\rangle)}{\sqrt{2}}$	4(c)
Step3	$ output\rangle = (H_n \otimes I) \psi_2\rangle = \sum_{j_1, \dots, j_n} a_{j_1 \dots j_n} j_1 \dots j_n\rangle \otimes \frac{(0\rangle - 1\rangle)}{\sqrt{2}}$	4(d)

with $a_{j_1 \dots j_n} = \frac{1}{2^n} \sum_{i_1, \dots, i_n} (-1)^{f(i_1, \dots, i_n)} (-1)^{(i_1, \dots, i_n) \cdot (j_1, \dots, j_n)}$, where $(i_1, \dots, i_n) \cdot (j_1, \dots, j_n)$ denotes $(i_1 \wedge j_1) \oplus \dots \oplus (i_n \wedge j_n)$, being $i_1, \dots, i_n, j_1, \dots, j_n \in \{0,1\}$.

If f is constant then $a_0 = 1$ and a_j is null for all $j \neq 0$. If it is balanced function, then $a_0 = 0$. Therefore, if after performing measurement on vector $|output\rangle$ a basis vector is obtained in the form

$$|0\rangle \otimes |0\rangle \otimes \dots \otimes |0\rangle \otimes \underbrace{|Measurement\ basis\rangle}_{|0\rangle}$$

or

$$|0\rangle \otimes |0\rangle \otimes \dots \otimes |0\rangle \otimes \underbrace{|Measurement\ basis\rangle}_{|1\rangle}$$

the f is constant. Otherwise, it is balanced.

For example, let $n=3$ and f_1, f_2 be defined as in Table 3.

Table 3. Example of constant and balanced functions

$x \in \{0,1\}^3$	$f_1(x)$	$f_2(x)$
000	0	1
001	0	0
010	0	1
011	0	1
100	0	0
101	0	0
110	0	0
111	0	1

Consider two cases of quantum entanglement operators as

$$U_{F_1} = I_4 \quad (Case\ 1) \quad (5)$$

and U_{F_2} is written as a block matrix with $C = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ as follows:

$$U_{F_2} = \begin{pmatrix} C & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & I & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & C & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & C & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & I & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & I & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & I & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & C \end{pmatrix} \quad (Case\ 2) \quad (6)$$

The computation involved by these two operators is resumed in Table 4.

Shannon and von Neumann entropy. A vector in a Hilbert space of dimension 2^k acts as a classical information source if the measurement with respect to a given orthonormal basis is performed. The possible outputs are the 2^k basis vectors, each one with probability given by the squared modulus of its probability amplitude. More in general, given a vector

$$|\varphi\rangle = \sum_{i_1, \dots, i_n \in \{0,1\}} a_{i_1, \dots, i_n} |i_1\rangle \otimes \dots \otimes |i_n\rangle \quad (7)$$

in a Hilbert space of dimension 2^n .

Let $T = \{j_1, \dots, j_k\} \subseteq \{1, \dots, n\}$ and $\{1, \dots, n\} - T = \{l_1, \dots, l_{n-k}\}$. Define

$$|\psi\rangle\langle\psi|_T = \sum_{\substack{t_{j_1}, \dots, t_{j_k} \\ i_{j_1}, \dots, i_{j_k}}} b_{t_{j_1}, \dots, t_{j_k}}^{i_{j_1}, \dots, i_{j_k}} |i_{j_1}, \dots, i_{j_k}\rangle\langle t_{j_1}, \dots, t_{j_k}|, \quad (8)$$

where

$$b_{t_{j_1}, \dots, t_{j_k}}^{i_{j_1}, \dots, i_{j_k}} = \sum_{i_{i_1} = t_{i_1}, \dots, i_{i_{n-k}} = t_{i_{n-k}}} a_{i_{i_1}, \dots, i_{i_n}} a_{t_{i_1}, \dots, t_{i_n}}^* \quad (9)$$

Table 4. Deutsch-Jozsa QAG state dynamic

Step	State (Case 1)	State (Case 2)
Input	$ 000\rangle \otimes 1\rangle$	$ 000\rangle \otimes 1\rangle$
Step 1	$\left(\frac{ 0\rangle + 1\rangle}{\sqrt{2}} \right) \otimes \left(\frac{ 0\rangle + 1\rangle}{\sqrt{2}} \right) \otimes \left(\frac{ 0\rangle + 1\rangle}{\sqrt{2}} \right)$ $\otimes \underbrace{\left(\frac{ 0\rangle - 1\rangle}{\sqrt{2}} \right)}_{\text{Ancilla qubit}}$	$\left(\frac{ 0\rangle + 1\rangle}{\sqrt{2}} \right) \otimes \left(\frac{ 0\rangle + 1\rangle}{\sqrt{2}} \right) \otimes \left(\frac{ 0\rangle + 1\rangle}{\sqrt{2}} \right)$ $\otimes \underbrace{\left(\frac{ 0\rangle - 1\rangle}{\sqrt{2}} \right)}_{\text{Ancilla qubit}}$
Step 2	$\left(\frac{ 0\rangle + 1\rangle}{\sqrt{2}} \right) \otimes \left(\frac{ 0\rangle + 1\rangle}{\sqrt{2}} \right) \otimes \left(\frac{ 0\rangle + 1\rangle}{\sqrt{2}} \right)$ $\otimes \underbrace{\left(\frac{ 0\rangle - 1\rangle}{\sqrt{2}} \right)}_{\text{Ancilla qubit}}$	$\frac{- 000\rangle + 001\rangle - 010\rangle - 011\rangle + 100\rangle + 101\rangle + 110\rangle - 111\rangle}{\sqrt{2^3}}$ $\otimes \underbrace{\left(\frac{ 0\rangle - 1\rangle}{\sqrt{2}} \right)}_{\text{Ancilla qubit}}$
Step 3	$ 000\rangle \otimes \underbrace{\left(\frac{ 0\rangle - 1\rangle}{\sqrt{2}} \right)}_{\text{Ancilla qubit}}$	$\frac{ 010\rangle - 011\rangle - 100\rangle - 101\rangle}{\sqrt{2^3}} \otimes \underbrace{\left(\frac{ 0\rangle - 1\rangle}{\sqrt{2}} \right)}_{\text{Ancilla qubit}}$

Choosing T means selecting a subspace of the Hilbert space of $|\varphi\rangle$ in Eq. (7). If $T = \{j\}$, this subspace has dimension 2 and it is the subspace of the qubit j . Similarly, if $T = \{j_1, \dots, j_k\}$, the subspace of qubits is j_1, \dots, j_k . The density operator $|\psi\rangle\langle\psi|_T$ describes the projection of the density matrix corresponding to $|\psi\rangle$ on this subspace.

Define the Shannon entropy of T in $|\psi\rangle$ with respect to the basis $\mathcal{B} = \{|i_1\rangle \otimes \dots \otimes |i_n\rangle\}$ as

$$E_T^{Sh}(|\psi\rangle) = - \sum_{i=1}^{2^k} [|\psi\rangle\langle\psi|_T]_{i,i} \log_2 [|\psi\rangle\langle\psi|_T]_{i,i} \quad (10)$$

The Shannon entropy of T expresses the mean information gained by measuring the projection of $|\psi\rangle$ with respect to the projections of the vectors in \mathcal{B} on the subspace of the qubits in T . The Shannon entropy can be interpreted as the degree of disorder involved by vector $|\psi\rangle$ when the qubits in T are measured. Vector $|\psi\rangle$ does not act only as a classical information source. On the contrary, it stores also information in a non-local correlation that is through entanglement. In order to measure the quantity of entanglement of a set $T = \{j_1, \dots, j_k\}$ of qubits in $|\psi\rangle$ the Von Neumann entropy of T in $|\psi\rangle$ as following

$$E_T^{vN} = -\text{Tr}(|\psi\rangle\langle\psi|_T \log_2 |\psi\rangle\langle\psi|_T). \quad (11)$$

is used.

The von Neumann entropy of the qubits in T is interpreted as the measure of the degree of entanglement of these qubits with the rest of the system.

Information analysis of Deutsch-Jozsa QAG Before ${}^{n+1}H$ is applied, the input vector defined in Eq. (7) is such that for every qubit j as follows:

$$E_{\{j\}}^{Sh}(|input\rangle) = E_{\{j\}}^{vN}(|input\rangle) = 0 \quad (12)$$

Eq. (12) is easily proved by observing that

$$|input\rangle\langle input|_{\{j\}} = |0\rangle\langle 0| \quad (13)$$

for the first n qubits and

$$|input\rangle\langle input|_{\{n+1\}} = |1\rangle\langle 1| \quad (14)$$

Since $\log_2 1 = 0$ and both $\log_2 |0\rangle\langle 0|$ and $\log_2 |1\rangle\langle 1|$ correspond to the null squared matrix of order 2, the values for Shannon and von Neumann entropy are 0 for every qubit from Eq. (10) and Eq. (11).

When ${}^{n+1}H$ is applied [Step 1, Eq. (4 (b))], every qubit undergoes a unitary change of basis through the operator H . This means

$$|\psi_1\rangle\langle\psi_1|_{\{j\}} = H^{-1}(|input\rangle\langle input|_{\{j\}})H \quad (15)$$

Eq. (15) can be rewritten as

$$\forall j \in \{1, \dots, n\} : |\psi_1\rangle\langle\psi_1|_{\{j\}} = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \quad (16)$$

and

$$|\psi_1\rangle\langle\psi_1|_{\{n+1\}} = \frac{1}{2} \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}, \quad (17)$$

since it is known that von Neumann entropy is left unchanged by a unitary change of basis, then

$$E_{\{j\}}^{Sh}(|\psi_1\rangle) = 1, \quad E_{\{j\}}^{vN}(|\psi_1\rangle) = 0 \quad (18)$$

for all qubits j .

The application of the operator U_F [Step 2, Eq. (4 (c))] leaves the situation unchanged for qubit $n+1$, whereas it entangles the first qubits:

$$\forall j \in \{1, \dots, n\} : |\psi_2\rangle\langle\psi_2|_{\{j\}} = \frac{1}{2} \begin{pmatrix} 1 & \alpha_j \\ \alpha_j & 1 \end{pmatrix} \quad (19)$$

where

$$\alpha_j = \sum_{i_1, \dots, i_{j-1}, i_{j+1}, \dots, i_n} \frac{(-1)^{\sum_{i_j} f(i_1, \dots, i_n)}}{2^{n-1}}. \quad (20)$$

From the structure of the matrix in Eq. (19) the elements on the main diagonal are the same as in Eq. (16). This means the Shannon entropy has not changed. Moreover,

$$H^{-1}(|\psi_2\rangle\langle\psi_2|_{\{j\}})H = \frac{1}{2} \begin{pmatrix} 1 + \alpha_j & 0 \\ 0 & 1 - \alpha_j \end{pmatrix}. \quad (21)$$

Since von Neumann entropy is left unchanged by a unitary change, for the first n qubits

$$E_{\{j\}}^{Sh}(|\psi_2\rangle) = 1 \quad (22)$$

and

$$E_{\{j\}}^{vN}(|\psi_2\rangle) = \frac{1+\alpha_j}{2} \log_2 \frac{2}{1+\alpha_j} + \frac{1-\alpha_j}{2} \log_2 \frac{2}{1-\alpha_j}. \quad (23)$$

Finally, when ${}^n H \otimes I$ is applied [Step 3, Eq. (4d)], qubit $n+1$ is left unchanged again, whereas all other qubits undergo a unitary change of basis again through operator H . From Eq. (21), the Shannon and Von Neumann entropy are calculated as:

$$E_{\{j\}}^{Sh}(|output\rangle) = E_{\{j\}}^{vN}(|output\rangle) = \frac{1+\alpha_j}{2} \log_2 \frac{2}{1+\alpha_j} + \frac{1-\alpha_j}{2} \log_2 \frac{2}{1-\alpha_j}. \quad (24)$$

Since in general

$$E_{\{j\}}^{Sh}(|output\rangle) \geq E_{\{j\}}^{vN}(|output\rangle). \quad (25)$$

the action of $H_n \otimes I$ is to preserve the von Neumann entropy and to reduce the Shannon entropy of the first n qubits as much as possible. The two operators represented in Table 4 produce the information flow shown in Table 5.

In Case 2, the von Neumann entropy is maximal for every qubits and, therefore, it is not possible for the interference operator to reduce the Shannon entropy.

Table 5. Deutsch-Jozsa QAG information flow ($1 \leq j \leq 3$)

Step	Case 1		Case 2	
	$E_{\{j\}}^{Sh}(\psi\rangle)$	$E_{\{j\}}^{vN}(\psi\rangle)$	$E_{\{j\}}^{Sh}(\psi\rangle)$	$E_{\{j\}}^{vN}(\psi\rangle)$
Input	0, 0, 0	0, 0, 0	0, 0, 0	0, 0, 0
Step 1	1, 1, 1	0, 0, 0	1, 1, 1	0, 0, 0
Step 2	1, 1, 1	0, 0, 0	1, 1, 1	1, 1, 1
Step 3	0, 0, 0	0, 0, 0	1, 1, 1	1, 1, 1

From this analysis, the following conclusions can be drawn:

1	When the QA computation starts, the Shannon entropy coincides with the Von Neumann entropy, but they are both null.
2	The superposition operator increases the Shannon entropy of each qubit to its maximum, but leaves the von Neumann entropy unchanged.
3	The entanglement operator increases the von Neumann entropy of each qubit according to the property of the function f , but leaves the Shannon entropy unchanged.
4	The interference operator does not change the value of the von Neumann entropy introduced by the entanglement operator, but decreases the value of the Shannon entropy to its minimum, that is, to the value of the von Neumann entropy itself.

Intelligent output states of Deutsch-Jozsa algorithm. The von Neumann entropy is interpreted as the degree of information in a vector (describing the property of function f), namely as a measure of the information stored in quantum correlation about the function f . The Shannon entropy must be interpreted as the measure of the degree of inaccessibility to this information through the measurement. In this context, the QAG G of Eq. (3) transfers information from f into the output vector minimizing the quantity of unnecessary noise producible by the measurement, or, more technically, minimizing according to Eq. (25) and Eq. (3) the non-negative quantity:

$$N_{\{j\}}(|output\rangle) = E_{\{j\}}^{Sh}(|output\rangle) - E_{\{j\}}^{vN}(|output\rangle)$$

for the first n qubits. The measure of intelligence of an output state according to the definition in Eq. (0) is

$$\mathcal{I}(|output\rangle) = 1 - \langle N(|output\rangle) \rangle \quad (26)$$

where

$$\langle N(|output\rangle) \rangle = \frac{1}{n} \sum_{j \in \{1, \dots, n\}} N_{\{j\}}(|output\rangle) \quad (27)$$

is the mean unnecessary noise. According to this definition, the action of the Walsh-Hadamard transform in Deutsch-Jozsa algorithm is to associate to every possible function f a maximally intelligent output state, namely a state $|output\rangle$ such that

$$\mathcal{I}(|output\rangle) = 1.$$

Physically, the measure of intelligent QA, described by Eq. (26), characterizes the amount of value information necessary for decision making regarding successful solution of the QA.

Figs 1(a) and 1(b) show the measure of intelligent QA for two cases in Eqs (5) and (6) according to Eq.(26).

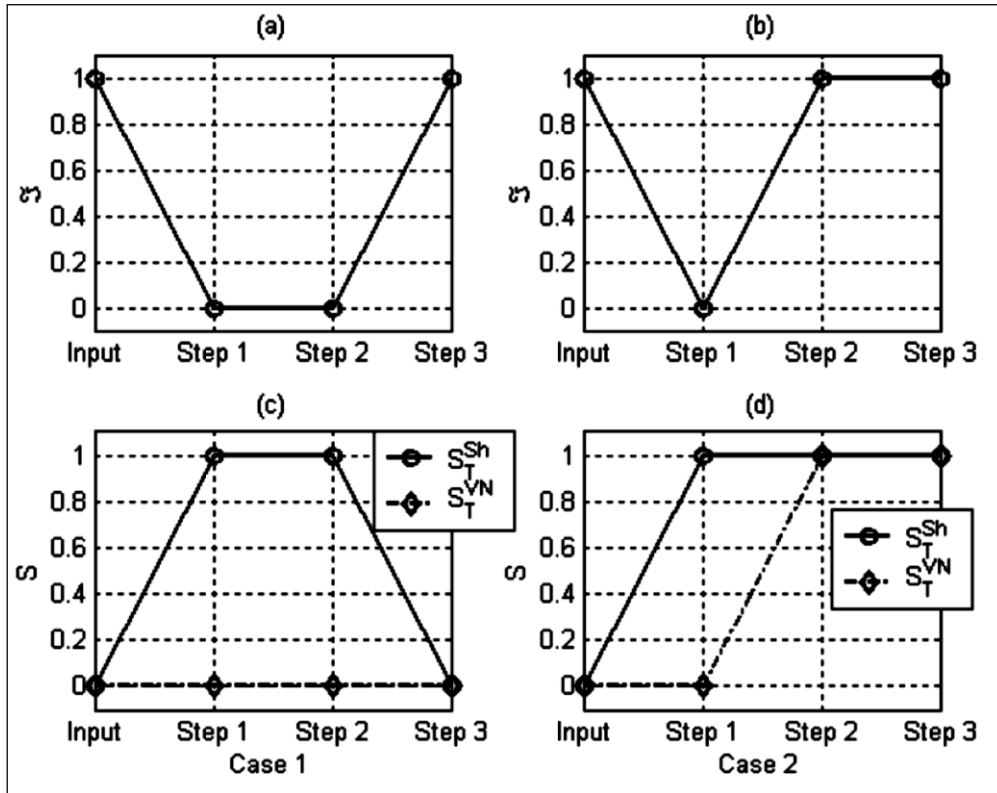


Figure 1. Measure of intelligence for Deutsch-Jozsa's QA for two cases from Table 3

In both cases this measure has the maximal value, i.e., equal to 1. It means that Deutsch-Jozsa QA as decision-making algorithm is intelligent QA with maximum degree 1. From Eq. (25), although optimality is fulfilled for the intelligence of the output states, the von Neumann entropy is still a lower bound for the Shannon entropy (see Figs 1 (c, d)). If the von Neumann entropy is too high, even a maximally intelligent output state may be «too random» when the measurement is performed.

Therefore, in Deutsch-Jozsa algorithm the information transfer from f into the output state is done by paying attention that the quantity of entanglement does not exceed. The role of «entanglement controller» is played by the pair «superposition-entanglement» operators. In order to illustrate this concept, consider the following matrix

$$U_F = \begin{pmatrix} C & 0 & 0 & 0 \\ 0 & I & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & C \end{pmatrix} \quad (28)$$

which encodes a balanced function for $n=2$. The von Neumann entropy of the first n qubits, when U_F is applied, is from Eq. (23)

$$E_{\{1\}}^{vN}(|\psi_2\rangle) = E_{\{2\}}^{vN}(|\psi_2\rangle) = \boxed{0} \quad (29)$$

If the role of the superposition was played by the operator ${}^nH \otimes I$ instead of ${}^{n+1}H$ and the input vector of dimension $n+1$ was

$$|input\rangle = |0\rangle \otimes |0\rangle \otimes \dots \otimes |0\rangle \otimes |0\rangle \quad (30)$$

then the von Neumann entropy for the first n qubits after the same step would be

$$E_{\{1\}}^{vN}(|\psi_2\rangle) = E_{\{2\}}^{vN}(|\psi_2\rangle) = \boxed{1}. \quad (31)$$

And, therefore, the Shannon entropy could not be reduced by the interference operator. The output would be completely random and the algorithm would not work.

Now consider similar examples with $n=3$ and f_1, f_2 be defined as in Table 1 for different entanglement operators that illustrate additional properties of information flows from the Deutsch-Jozsa QA.

Let $n=3$ and f_1, f_2 be defined as in Table 1 and consider two additional cases of quantum entanglement operators as

$$U_{F_3} = \begin{pmatrix} I & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & C & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & I & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & C & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & C & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & C \end{pmatrix} (Case 3) \quad (32)$$

and U_{F_2} is written as a block matrix as follows:

$$U_{F_4} = I_2 \otimes \begin{pmatrix} I & 0 \\ 0 & C \end{pmatrix} (Case 4) \quad (33)$$

Tables 6 and 7 show the dynamics of the Deutsch-Jozsa algorithm for the Cases 3 and 4, correspondingly.

For comparison of results Table 8 shows the results of calculation for the Case 1.

Table 6. Information Analysis of Deutsch-Jozsa's Algorithm for case 3

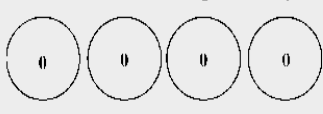
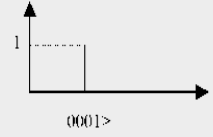

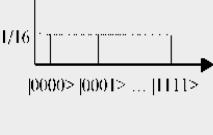
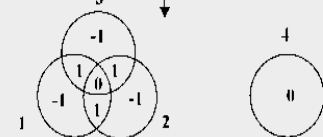

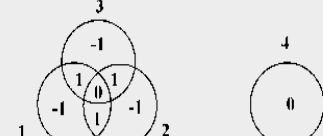
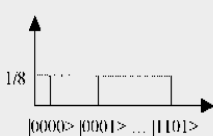
Step	Classical Entropy $H_{sh}(\{\psi\})$	Quantum Entropy $S_{\psi}(\{j\})$	States and Gate Operations	Dynamics of Solution Probabilities
Input	0		$ 000\rangle \otimes 1\rangle$ \xrightarrow{H}	
Superposition	$(1,1,1,1)$ 4		$\frac{ 0\rangle+ 1\rangle}{\sqrt{2}} \otimes \frac{ 0\rangle+ 1\rangle}{\sqrt{2}} \otimes \frac{ 0\rangle- 1\rangle}{\sqrt{2}} \otimes \frac{ 0\rangle- 1\rangle}{\sqrt{2}}$ $\xrightarrow{U_F}$	
Entanglement	$(1,1,1,1)$ 4		$\frac{1}{2\sqrt{2}} \left(000\rangle - 001\rangle + 010\rangle + 011\rangle + 100\rangle - 101\rangle - 110\rangle - 111\rangle \right) \otimes \frac{ 0\rangle- 1\rangle}{\sqrt{2}}$ $\xrightarrow{H \otimes I}$	
Interference	$(1,1,1,0)$ 3		$\frac{1}{2} \left(001\rangle + 011\rangle - 100\rangle - 110\rangle \right) \otimes \frac{ 0\rangle- 1\rangle}{\sqrt{2}}$	

Table 7. Information Analysis of Deutsch-Jozsa's Algorithm for case 4

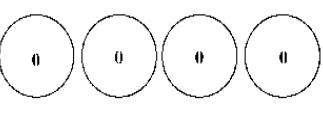
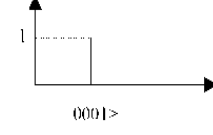
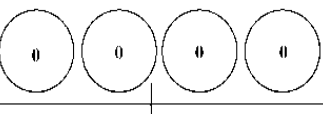
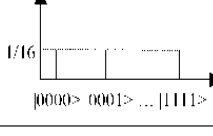

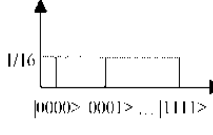
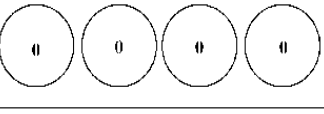
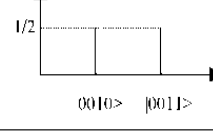
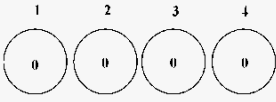


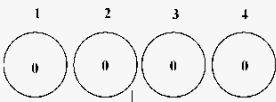

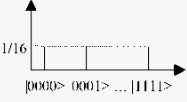
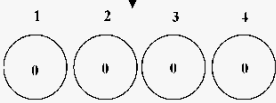

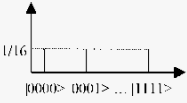
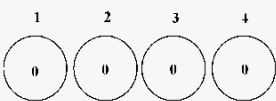

Step	Classical Entropy $H_{sh}(\{\psi\})$	Quantum Entropy $S_{\psi}(\{j\})$	States and Gate Operations	Dynamics of Solution Probabilities
Input	0		$ 000\rangle \otimes 1\rangle$ \xrightarrow{H}	
Superposition	$(1,1,1,1)$ 4		$\frac{ 0\rangle+ 1\rangle}{\sqrt{2}} \otimes \frac{ 0\rangle+ 1\rangle}{\sqrt{2}} \otimes \frac{ 0\rangle- 1\rangle}{\sqrt{2}} \otimes \frac{ 0\rangle- 1\rangle}{\sqrt{2}}$ $\xrightarrow{U_F}$	
Entanglement	$(1,1,1,1)$ 4		$\frac{ 0\rangle+ 1\rangle}{\sqrt{2}} \otimes \frac{ 0\rangle+ 1\rangle}{\sqrt{2}} \otimes \frac{ 0\rangle- 1\rangle}{\sqrt{2}} \otimes \frac{ 0\rangle- 1\rangle}{\sqrt{2}}$ $\xrightarrow{H \otimes I}$	
Interference	$(0,0,1,0)$ 1		$ 001\rangle \otimes \frac{ 0\rangle- 1\rangle}{\sqrt{2}}$	

Table 8. Information Analysis of Deutsch-Jozsa's Algorithm for case 1

Step	Classical Entropy $H_{sh}(\psi)$	Quantum Entropy $S_{\psi}(\{j\})$	States and Gate Operations	Dynamics of Solution Probabilities
Input	0		$ 000\rangle \otimes 1\rangle$ 	
Super-position	$(1,1,1,1)$ 4		$\frac{ 0\rangle+ 1\rangle}{\sqrt{2}} \otimes \frac{ 0\rangle+ 1\rangle}{\sqrt{2}} \otimes \frac{ 0\rangle- 1\rangle}{\sqrt{2}} \otimes \frac{ 0\rangle- 1\rangle}{\sqrt{2}}$ 	
Entanglement	$(1,1,1,1)$ 4		$\frac{ 0\rangle+ 1\rangle}{\sqrt{2}} \otimes \frac{ 0\rangle+ 1\rangle}{\sqrt{2}} \otimes \frac{ 0\rangle- 1\rangle}{\sqrt{2}} \otimes \frac{ 0\rangle- 1\rangle}{\sqrt{2}}$ 	
Interference	$(0,0,0,0)$ 0		$ 000\rangle \otimes \frac{ 0\rangle- 1\rangle}{\sqrt{2}}$	

By applying the above mentioned information analysis to these three tables, one can draw the following physical interpretation of results and conclusions about classical and quantum entropy, changing after superposition, entanglement and interference have taken place:

1	The input vector is a basis vector, therefore, the classical information of this state is 0; it is the tensor product of n basis vectors of dimension 2, so the von Neumann entropy of every qubits composing it is also 0	
2	The superposition operator H_4 increase the classical Shannon entropy its minimal value 0 to its maximal value 4, but leaves the situation unchanged from the quantum von Neumann entropy point of view	
3	The entanglement operator is a classical unitary operator therefore it maps different basis vectors into different basis vectors leaving the classical information on the system unchanged. On the contrary it may create correlation among the different binary vectors in the tensor product describing the system state; this correlation is described by the von Neumann entropy of the different subparts of the system:	
	3.a	The quantum information of the whole system is always 0, even when entanglement operator creates correlation, since the vector describing it is a pure state, whereas inner values for mutual information and conditional entropy may be positive or negative: they encode the quantum information necessary to decode the property being investigated for operator of entanglement U_F
	3.b	The states of the system before and after action of the entanglement operator takes place cannot be distinguished from a classical information point of view, since the Shannon entropy did not change. Only with a quantum information approach is the difference between these two states can be revealed
4	The interference operator leaves the quantum information picture unchanged maintaining encoded the information necessary to identify U_F as a constant or balanced operator. On the contrary, it decreases the classical entropy making quantum information accessible; through the action of interference the vector acquires the minimum of classical entropy: such a vector according to the definition is an intelligent state because it represents a coherent output of QA computation with minimum entropy uncertainty relation (EUR) as successful result	

A comparison of Tables 6 and 7 reveals that:

- The entanglement operator in Case 3 effectively creates quantum correlation among different sub-parts of the system, whereas in Case 4 the general state is written as the tensor product of binary basis vectors and so no quantum correlation is involved;
- The interference operator in Case 3 reduces the classical Shannon entropy of 1 bit, whereas in Case 4 it reduces it of 3 bits.
- This explains why it is important to choose carefully both the superposition operator and the input vector in order to store in quantum correlation the information actually needed to solve the problem.
- The following general properties are observed for the Deutsch-Jozsa algorithm:

1	The presence of quantum correlation appears as the degree of resistance (immunity) of the system to change its classical entropy, as the measure of state chaos and defines the internal degree of intelligent possibility of QA
2	The action of interference undergoes this property mapping U_F into an intelligent state revealing it

Now consider from Table 8 the results of simulation for Case 1. In this situation, the entanglement operator creates no correlation. This is a common characteristic to all linear operators U_F implementing a function $f: \{0,1\}^n \rightarrow \{0,1\}^m$ such that $f(x) = k \cdot x$ or $f(x) = \neg(k \cdot x)$ for some binary constant k , as it showed in Table 9.

These functions among the input set of balanced and constant minimize to 0 the «gap» between the highest and lowest information values appearing in the Wenn-diagram of shown in the tables. Other balanced functions are mapped into less intelligent states that are higher classical entropy vectors.

This means that it is a non-success result as it is shown in Table 10.

Table 9. Information Analyses of Deutsch-Jozsa's Algorithm (Linear Functions)

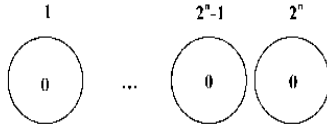
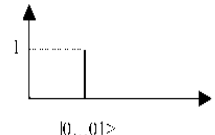
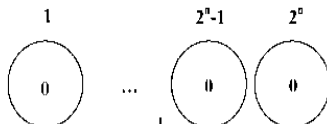
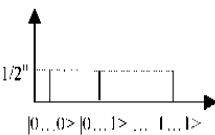
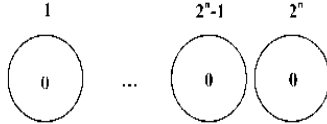
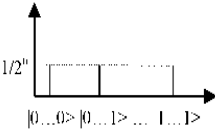
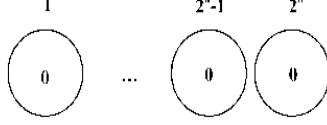
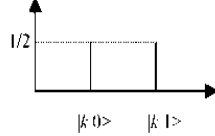
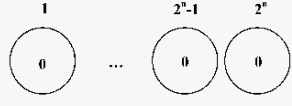

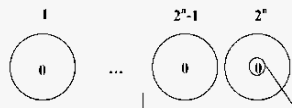

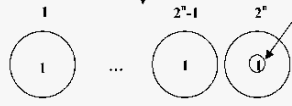

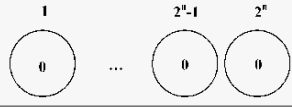

Step	Classical Entropy $H_{Sh}(\psi)$	Quantum Entropy $S_{\psi}(\{j\})$	States and Gate Operations	Dynamics of Solution Probabilities
Input	0		$ 0\dots 0\rangle \otimes 1\rangle$ \xrightarrow{H}	
Superposition	$n+1$		$\frac{ 0\rangle+ 1\rangle}{\sqrt{2}} \otimes \dots \otimes \frac{ 0\rangle+ 1\rangle}{\sqrt{2}} \otimes \frac{ 0\rangle- 1\rangle}{\sqrt{2}}$ $\xrightarrow{U_F}$	
Entanglement	$n+1$		$\frac{ 0\rangle \pm 1\rangle}{\sqrt{2}} \otimes \dots \otimes \frac{ 0\rangle \pm 1\rangle}{\sqrt{2}} \otimes \frac{ 0\rangle - 1\rangle}{\sqrt{2}}$ $\xrightarrow{H \otimes I}$	
Interference	1		$ k\rangle \otimes \frac{ 0\rangle - 1\rangle}{\sqrt{2}}$	

Table 10. Information Analysis of Deutsch-Jozsa's Algorithm
(Non-Linear Balanced Functions)

Step	Classical Entropy $H_{sn}(\psi)$	Quantum Entropy $S_{\psi}(\{j\})$	States and Gate Operations	Dynamics of Solution Probabilities
Input	0		$ 0 \dots 0\rangle \otimes 1\rangle$ \xrightarrow{H}	
Superposition	$n+1$		$\frac{ 0\rangle - 1\rangle}{\sqrt{2}} \otimes \dots \otimes \frac{ 0\rangle - 1\rangle}{\sqrt{2}} \otimes \frac{ 0\rangle - 1\rangle}{\sqrt{2}}$ $\xrightarrow{U_f}$	
Entanglement	$n+1$		$\psi \otimes \frac{ 0\rangle - 1\rangle}{\sqrt{2}}$ $\xrightarrow{H \otimes I}$	
Interference	$S^{sn} > 1$		$ \mu\rangle \otimes \frac{ 0\rangle - 1\rangle}{\sqrt{2}}$	

The Deutsch-Jozsa's QA undergoes the special structure of its input set of functions from a quantum information point of view. This structure is pictured in Fig. 2.

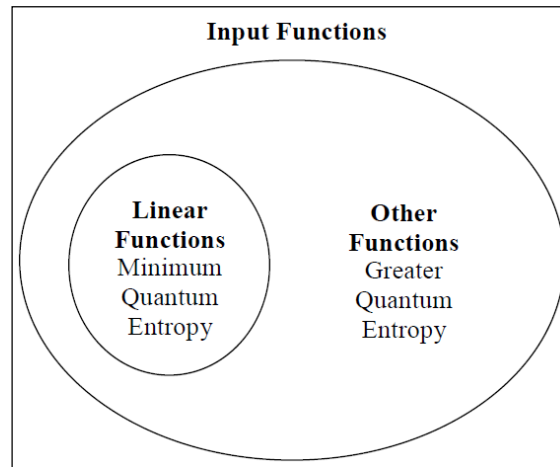


Figure 2. Quantum Information Structure of Deutsch-Jozsa's Input Space

On the analysis level of the Deutsch-Jozsa algorithm, the next step is to investigate the relationship between the von Neumann entropy introduced by the entanglement operator and the problem the algorithm solves. It is possible to quantify the information about a given function that is sufficient to store in the system in order to decide if it is constant or balanced. More in general, the same information analysis carried on for Deutsch-Jozsa algorithm should be done for the other QA's benchmarks in order to have a global picture of the known quantum information processing techniques.

Information analysis of Shor's quantum search algorithm: The information role of entanglement and interference in Shor's QAG

The above-mentioned technique from quantum information theory can be used in the domain of QA synthesis and simulation. For this purpose, the classical and quantum information flow in the Shor's QA is analyzed. The QAG G , which is based on superposition, quantum supercorrelation (entanglement) and interference, when acting on the input vector, stores information into the system state, and in this case (similar

to Deutsch-Jozsa QA case) minimizing the gap between the classical Shannon entropy and the quantum von Neumann entropy. This principle provides both a methodology to design a QG and a technique to efficiently simulate its behavior on a classical computer.

In Shor's algorithm, the dynamics of quantum computation states are analyzed from the classical and quantum information points of view. The Shannon entropy is interpreted (as mentioned above) as the degree of information accessibility through measurement, while the von Neumann entropy is employed to measure the quantum information of entanglement. The intelligence of a state with respect to a subset of qubits in accordance with Eq. (0) is defined. Similar to abovementioned results with Deutsch-Jozsa QA, the intelligence of a state is maximal if the gap between the Shannon and the von Neumann entropy for the chosen result qubits is minimal. The quantum Fourier transform (QFT) creates maximally intelligent states with respect to the first n qubits for Shor's problem, since it annihilates the gap between the classical and quantum entropies for the first n qubits of every output states.

Computational dynamics of Shor's QA-gate (QAG) In the Shor's algorithm an integer number $n > 0$ and a function $f: \{0,1\}^n \rightarrow \{0,1\}^n$ are given such that f have period r , namely f is such that $\forall x \in \{0,1\}^n : f(x) \equiv f(x+r) \bmod n$, and f is injective with respect to its period. The problem is to find r .

The function f is first encoded into the injective function

$$F: \{0,1\}^n \times \{0,1\}^n \rightarrow \{0,1\}^n \times \{0,1\}^n$$

such that:

$$F\{x, y\} = (x, y \oplus f(x)) \quad (34)$$

where \oplus is the bitwise XOR operator. F is then encoded into a unitary operator U_F . This purpose is fulfilled by mapping every binary input string of length $2n$ into a vector in a Hilbert space of dimension 2^{2n} according to the following recursive encoding scheme τ :

$$\tau(0) = |0\rangle \quad \tau(0) = |0\rangle \quad \tau(z_1 \dots z_{2n}) = |z_1 \dots z_{2n}\rangle \quad (35)$$

where $|z_1 \dots z_{2n}\rangle$ stands for the tensor product $|z_1\rangle \otimes \dots \otimes |z_{2n}\rangle$, being $z_1, \dots, z_{2n} \in \{0,1\}$.

Each bit value in a string is mapped into a vector of a Hilbert sub-space of dimension 2 . This subspace is called a qubit. Similarly, a sequence f successive bit values of length l is mapped into a vector of dimension 2^l . This subspace is a quantum register of length l . Using this scheme, the operator U_F is defined as a squared matrix of order 2^{2n} such that:

$$\forall z \in \{0,1\}^{2n} : U_F |z\rangle = |F(z)\rangle. \quad (36)$$

Practically, the operator U_F is as follows:

$$[U_F]_{i,j} = \delta_{i, 1 + [F([j-1]_{(2)})]_{(10)}} \quad (37)$$

where $[q]_{(b)}$ is the basis b representation of number q and $\delta_{i,j}$ is the Kronecker delta.

The idea of encoding a function f into unitary operator is not a peculiarity of the Shor's algorithm, but it is typical of all known QA's. In general, U_F contains the information about the function f needed to solve the problem.

In the Shor's case, one could calculate the period r of f by testing the operator U_F on the input vectors $\underbrace{|0 \dots 0\rangle}_n \otimes \underbrace{|0 \dots 0\rangle}_n$ obtaining $\underbrace{|0 \dots 0\rangle}_n \otimes \underbrace{|f(0 \dots 0)\rangle}_n$, $\underbrace{|0 \dots 1\rangle}_n \otimes \underbrace{|0 \dots 0\rangle}_n$ obtaining $\underbrace{|0 \dots 1\rangle}_n \otimes \underbrace{|f(0 \dots 1)\rangle}_n$ and so on until a vector $\underbrace{|x_1 \dots x_n\rangle}_n$ for the first register of length n is found such that the corresponding vector

$\underbrace{|f(x_1 \dots x_n)\rangle}_n$ in the second register of length n coincides with $\underbrace{|f(0 \dots 0)\rangle}_n$. The period r of f coincides with the binary number $x_1 \dots x_n$. The number of U_F tests required by this algorithm is r .

Since the period r of the function varies from 1 to 2^n , the temporal complexity of this algorithm is exponential for the worst case. In order to extract the information stored in U_F more effectively, a different perspective is used. The operator U_F must in fact be used in order to transfer as much information as possible from operator to the input vector each time U_F works. To this purpose, it is embedded into a unitary operator G , called the QAG, having the following general form:

$$G = (IF \otimes I_m) \cdot U_F \cdot (IF \otimes I_m) \quad (38)$$

where IF stands for a unitary squared matrix of order 2^n and I_m for identity matrix of order 2^n . In the case of the Shor's algorithm, U_F is embedded into the unitary QAG (see Table 3.1)

$$G = (QFT_n \otimes I_n) \cdot U_F \cdot (QFT_n \otimes I_n). \quad (39)$$

The symbol QFT_n denotes the unitary quantum Fourier transform of order n :

$$[QFT_n]_{ij} = \frac{1}{2^{n/2}} \exp \left\{ 2\pi J \left[\frac{(i-1)(j-1)}{2^n} \right] \right\}, \quad (40)$$

where J is the imaginary unit. Subsequently, the gate does not act on many different basis input vectors. On the contrary, it always gets as input the starting vector $\underbrace{|0 \dots 0\rangle}_n \otimes \underbrace{|0 \dots 0\rangle}_n$.

The corresponding computation evolves according to the following steps:

Step	Computational algorithm	Equation
Step 0	$ input\rangle = \underbrace{ 0 \dots 0\rangle}_n \otimes \underbrace{ 0 \dots 0\rangle}_n$	(41)
Step 1	$ \psi_1\rangle = (QFT_n \otimes I_n) input\rangle = \frac{1}{2^{n/2}} \sum_{i_1, \dots, i_n} i_1 \dots i_n\rangle \otimes \underbrace{ 0 \dots 0\rangle}_n$	(42)
Step 2	$ \psi_2\rangle = U_F \psi_1\rangle = \frac{1}{2^{n/2}} \sum_{i_1, \dots, i_n} i_1 \dots i_n\rangle \otimes \underbrace{ f(i_1 \dots i_n)\rangle}_n$	(43)
Step 3	$ output\rangle = (QFT_n \otimes I_n) \psi_2\rangle = \frac{1}{2^{n/2}} \sum_{\substack{j_1, \dots, j_n \\ i_1, \dots, i_n}} a_{i_1 \dots i_n}^{j_1 \dots j_n} j_1 \dots j_n\rangle \otimes \underbrace{ f(i_1 \dots i_n)\rangle}_n$	(44)

where $a_{i_1 \dots i_n}^{j_1 \dots j_n} = \frac{1}{2^{n/2}} \exp \left\{ 2\pi J \left[\frac{(i_1, \dots, i_n)_{(10)} (j_1, \dots, j_n)}{2^n} \right] \right\}.$

If $k = \frac{2^n}{r}$ is an integer number, the output state can be written as

$$|output\rangle = \frac{1}{r} \sum_{p=0}^{r-1} \sum_{s=0}^{r-1} \exp \left\{ 2\pi J s [i_1 \dots i_n]_{(10)} \frac{l_p}{r} \right\} \left| \left[\frac{s 2^n}{r} \right]_{(2)} \right\rangle \otimes |[p]_{(2)}\rangle, \quad (45)$$

where l_p is an integer positive number and binary representation are obtained using n bits. Therefore, the first quantum register of length n of the output state generates a periodical probability distribution with period k for every possible vector of the second register. By repeating the algorithm a number of times polynomial in n and by performing a measurement each time, one can reconstruct the value of r .

Physical interpretation of Shor's algorithm steps In Step 1 the operator $(QFT_n \otimes I)$ acts on a basis vector. It transforms the vector source $\underbrace{|0\dots 0\rangle}_n \otimes \underbrace{|0\dots 0\rangle}_n$ into a linear combination of equally weighted basis vectors of the form $|i_1\dots i_n\rangle \otimes \underbrace{|0\dots 0\rangle}_n$. Since every basis vector is interpreted as a possible observable state of the system, the QFT_n plays the role of the superposition operator for the first n qubits.

In Step 3, the operator $(QFT_n \otimes I)$ acts on every basis vector belonging to the linear combination $|\psi_2\rangle$. This means that every vector of such a combination generates a superposition of basis vectors, whose complex weights (i.e., amplitudes of probability) are equal in modulus, but different in phase. Every basis vector is now weighted by the summation of the probability amplitudes coming from the different source vectors. This summation can increase or decrease the resulting amplitude of probability.

Since this phenomenon is very similar to classical wave interference, in Step 3, the operator QFT_n plays the role of the interference operator. From the mathematical point of view, when the matrix QFT_n acts as a superposition operator (Step 1), the first matrix column only is involved in the calculation of the resulting vector. On the contrary, when it acts for the second time (Step 3), all matrix columns are involved and the interference among the weights coming from the different source vectors takes place.

The operator U_F (Step 2) acts between the first and the second application of QFT_n . Its effect is to map every basis vector of $|\psi_1\rangle$ into another basis vector injectively. In this way it may create nonlocal correlation among qubits. Therefore, U_F plays the role of the entanglement operator.

The QAGs of the best known algorithms can all be described as the composition of a superposition, an entanglement, and interference operators, where the superposition and the interference operators coincide, but play different roles, as it is in the case for QFT_n in the above Step 1 and Step 3. From a qualitative point of view, the action of the superposition operator is to exploit the potential parallelism of the system by preparing the system itself in a superposition of all its possible states. When the entanglement operator acts on this superposed state the whole information about f contained in U_F is transferred to the resulting vector. Finally, the interference operator makes this information accessible by measurement in order to solve the problem.

To illustrate this, consider, for example, Shor's algorithm with $n=3$ and f_1, f_2 defined as in Table 11.

Table 11. Example of periodical functions

x	$f_1(x)$	$f_2(x)$
000	001	000
001	111	010
010	001	100
011	111	110
100	001	000
101	111	010
110	001	100
111	111	110

Then

$$U_{F_1} = I_2 \otimes \begin{pmatrix} I_2 & 0 \\ 0 & C_2 \end{pmatrix} \otimes C \quad (\text{Case 1}) \quad (46)$$

and

$$U_{F_2} = I \otimes \begin{pmatrix} I_2 & 0 & 0 & 0 \\ 0 & I \otimes C & 0 & 0 \\ 0 & 0 & C \otimes I & 0 \\ 0 & 0 & 0 & C_2 \end{pmatrix} \otimes I, C = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (\text{Case2}). \quad (47)$$

The computation involved with these two cases of operators is shown in Table 12 and Table 13.

Table 12. Shor's QG information flow with $f = f_1$

Step	State
Input	$ 000\rangle \otimes 000\rangle$
Step 1	$\frac{(0\rangle + 1\rangle)}{\sqrt{2}} \otimes \frac{(0\rangle + 1\rangle)}{\sqrt{2}} \otimes \frac{(0\rangle + 1\rangle)}{\sqrt{2}} \otimes 000\rangle$
Step 2	$\frac{(0\rangle + 1\rangle)}{\sqrt{2}} \otimes \frac{(0\rangle + 1\rangle)}{\sqrt{2}} \otimes \frac{(000\rangle + 111\rangle)}{\sqrt{2}} \otimes 1\rangle$
Step 3	$\frac{1}{\sqrt{2}} \left(\frac{(0\rangle + 1\rangle)}{\sqrt{2}} \otimes 0000\rangle + \frac{(0\rangle - 1\rangle)}{\sqrt{2}} \otimes 0011\rangle \right) \otimes 1\rangle$

Table 13. Shor's QG information flow with $f = f_2$

Step	State
Input	$ 000\rangle \otimes 000\rangle$
Step 1	$\frac{(0\rangle + 1\rangle)}{\sqrt{2}} \otimes \frac{(0\rangle + 1\rangle)}{\sqrt{2}} \otimes \frac{(0\rangle + 1\rangle)}{\sqrt{2}} \otimes 000\rangle$
Step 2	$\frac{(0\rangle + 1\rangle)}{\sqrt{2}} \otimes \frac{1}{2} (0000\rangle + 0101\rangle + 1010\rangle + 1111\rangle) \otimes 0\rangle$
Step 3	$\frac{1}{\sqrt{2}} \left(000\rangle \otimes \frac{(0\rangle + 1\rangle)}{\sqrt{2}} \otimes \frac{(0\rangle + 1\rangle)}{\sqrt{2}} + 010\rangle \otimes \frac{(0\rangle - 1\rangle)}{\sqrt{2}} \otimes \frac{(0\rangle - 1\rangle)}{\sqrt{2}} \right. \\ \left. + 100\rangle \otimes \frac{(0\rangle + 1\rangle)}{\sqrt{2}} \otimes \frac{(0\rangle - 1\rangle)}{\sqrt{2}} + 110\rangle \otimes \frac{(0\rangle - 1\rangle)}{\sqrt{2}} \otimes \frac{(0\rangle - 1\rangle)}{\sqrt{2}} \right) \otimes 0\rangle$

Information analysis of the Shor's QAG To understand how the intelligence of $|\psi\rangle$ changes while the Shor's algorithm runs the set of the first n qubits, namely $T = \{1, \dots, n\}$ is considered for the case where 2^n is multiple of r .

The input vector defined in Eq. (4.41) is such that

$$E_T^{Sh}(|input\rangle) = E_T^{vN}(|input\rangle) = 0 \quad (48)$$

The intelligence of the state is:

$$\mathcal{J}(|input\rangle) = 1 \quad (49)$$

Eq. (48) is easily proved by observing that

$$|input\rangle\langle input|_T = |0\rangle\langle 0|_n \quad (50)$$

$(|0\rangle\langle 0|_n)$ is the n -th tensor power of $|0\rangle\langle 0|$. Since $\log_2 1 = 0$, $\log_2 |0\rangle\langle 0|_n$ corresponds to the null squared matrix of order 2^n . Then it follows from Eq. (42) and Eq. (42) that the value of $S_T^{Sh}(|input\rangle)$ and $S_T^{vN}(|input\rangle)$ are both 0. In other words, the input state belongs to the measurement basis \mathcal{B} , therefore, both its Shannon and von Neumann entropy with respect to T are zero.

When $(QFT_n \otimes I_n)$ is applied [Step 1, Eq. (42)], the first n qubits undergo a unitary change of basis. This means their von Neumann entropy is left unchanged. On the contrary, the Shannon entropy increases. From Eq. (42) the Shannon entropy value is obtained from the main diagonal values. This means that after Step 1 it is given by

$$E_T^{Sh}(|\psi_1\rangle) = n, \quad E_T^{vN}(|\psi_1\rangle) = 0 \quad (51)$$

The intelligence of the state with respect to the first n qubits is at this point $\mathcal{J}_T(|\psi_1\rangle) = 0$. The application of U_F (Step 2) entangles the first n qubits with the last n . In fact, being f periodical with period r and being $k = \frac{2^n}{r}$ an integer number, the state $|\psi_2\rangle$ can be written

$$|\psi_2\rangle = \sum_{l=0}^{r-1} \left(|l\rangle_{(2)} + |l+r\rangle_{(2)} + \left| l + \left(\frac{2^n}{r} - 1 \right) r \right\rangle_{(2)} \right) \otimes |f(l)\rangle. \quad (52)$$

From Eq. (52), the density matrix $|\psi_2\rangle\langle\psi_2|_T$ is written as a $k \times k$ block matrix

$$|\psi_2\rangle\langle\psi_2|_T = \frac{1}{2^n} \begin{pmatrix} I(r) & I(r) & \dots & I(r) \\ I(r) & I(r) & \dots & I(r) \\ \dots & \dots & \dots & \dots \\ I(r) & I(r) & \dots & I(r) \end{pmatrix}, \quad (53)$$

where $I(r)$ denotes the identity matrix of order r . The matrix $|\psi_2\rangle\langle\psi_2|_T$ can be decomposed into the tensor product of $1 + \log_2 k$ smaller density matrices:

$$|\psi_2\rangle\langle\psi_2|_T = \frac{1}{2^{\log_2 k}} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}_{\log_2 k} \otimes \frac{1}{r} I(r). \quad (54)$$

The von Neumann entropy of a tensor product can be written as the summation of the von Neumann entropies of its factors. Therefore:

$$S_T^{vN}(|\psi_2\rangle) = -(\log_2 k) Tr \left(\frac{1}{2} A \log_2 \left(\frac{1}{2} A \right) \right) - Tr \left(\frac{1}{r} I(r) \log_2 \left(\frac{1}{r} I(r) \right) \right), \quad (55)$$

where $A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$. Since $A/2$ is similar to $|1\rangle\langle 1|$ through a unitary change of basis, then Eq.(55) is written as

$$S_T^{vN}(|\psi_2\rangle) = -(\log_2 r) Tr(|1\rangle\langle 1| \log_2 |1\rangle\langle 1|) - Tr \left(\frac{1}{r} I_r \log_2 \left(\frac{1}{r} I_r \right) \right) = \boxed{\log_2 r}. \quad (56)$$

The first equality in Eq. (56) is obtained by noting that $Tr(|1\rangle\langle 1| \log_2 |1\rangle\langle 1|) = 0$. From the structure of the matrix in Eq. (53) it follows that the Shannon entropy did not change. Then for the set T of the first n qubits

$$S_T^{Sh}(|\psi_2\rangle) = n, \quad S_T^{vN}(|\psi_2\rangle) = \log_2 r. \quad (57)$$

This means that

$$\mathcal{J}_T(|\psi_2\rangle) = \frac{1}{n} \log_2 r. \quad (58)$$

Finally, when $(QFT_n \otimes {}^n I)$ is applied [Step 3, Eq. (44)], the last n qubits are left unchanged, whereas the first n qubits undergo a unitary change of basis through the QFT. This implies that the von Neumann entropy is reduced. Indeed, from Eq. (45), the input superposition of the first n qubits is periodic with period $k = \frac{2^n}{r}$ and only r different basis vectors can be measured, every one with probability $\frac{1}{r}$. This means

$$S_T^{Sh}(|output\rangle) = \log_2 r, \quad S_T^{vN}(|output\rangle) = \log_2 r. \quad (59)$$

The intelligence of the output state with respect to T is

$$\mathcal{J}_T(|output\rangle) = 1. \quad (60)$$

From Eq. (60) it follows that the QFT preserves the von Neumann entropy and the Shannon entropy of the first n qubits as much as possible.

The two operators represented in Table 9 produce the information flow reported in Table 14 and Table 15.

Table 14. Shor's QAG information flow with $f = f_1$

Step	$E_T^{Sh}(\psi\rangle)$	$E_T^{vN}(\psi\rangle)$	$\mathcal{J}_T(\psi\rangle)$
Input	0	0	1
Step 1	3	0	0
Step 2	3	1	$\frac{1}{3}$
Step 3	1	1	1

It is worth observing how the intelligence of the state increases and decreases while the algorithm evolves.

Information analysis of Shor's algorithm is presented in Table 16.

Table 15. Shor's QAG information flow with $f = f_2$

Step	$E_T^{Sh}(\psi\rangle)$	$E_T^{vN}(\psi\rangle)$	$\mathcal{J}_T(\psi\rangle)$
Input	0	0	1
Step 1	3	0	0
Step 2	3	2	$\frac{2}{3}$
Step 3	2	2	1

Now, for comparison, consider the case $n=2$ for the function f_2 with the period 4 and the entanglement operator as the particular case of Eq. (47).

$$U_{F_2} = \begin{pmatrix} I \otimes I & 0 & 0 & 0 \\ 0 & I \otimes C & 0 & 0 \\ 0 & 0 & C \otimes I & 0 \\ 0 & 0 & 0 & C \otimes I \end{pmatrix} \quad (\text{Case 3}) \quad (61)$$

Table 16. Information Analysis of Shor's Algorithm (case1, $f = f_1$) in Eq. (46)

Step	Classical Entropy $H_{sh}(\psi)$	Quantum Entropy $S_{\psi}(\{j\})$	States and Gate Operations	Dynamics of Solution Probabilities
Input	0		$ 000\rangle \otimes 000\rangle$ $\xrightarrow{{}^3H \otimes {}^3I}$	
Superposition	3		$\frac{ 0\rangle + 1\rangle}{\sqrt{2}} \otimes \frac{ 0\rangle + 1\rangle}{\sqrt{2}} \otimes \frac{ 0\rangle + 1\rangle}{\sqrt{2}} \otimes 000\rangle$ $\xrightarrow{U_F}$	
Entanglement	3		$\frac{ 0\rangle + 1\rangle}{\sqrt{2}} \otimes \frac{ 0\rangle + 1\rangle}{\sqrt{2}} \otimes \frac{ 000\rangle + 111\rangle}{\sqrt{2}} \otimes 1\rangle$ $\xrightarrow{QFT_3 \otimes I}$	
Interference	1		$\left[\frac{ 0\rangle + 1\rangle}{2} \otimes 0000\rangle + \frac{ 0\rangle - 1\rangle}{2} \otimes 0011\rangle \right] \otimes 1\rangle$	

Table 17 shows the evolution of the algorithm when applied with this operator.

Table 17. Information Analysis of Shor's Algorithm for case 3

Step	Classical Entropy $H_{sh}(\psi)$	Quantum Entropy $S_{\psi}(\{j\})$	States and Gate Operations	Dynamics of Solution Probabilities
Input	0		$ 00\rangle \otimes 00\rangle$ $\xrightarrow{{}^2H \otimes {}^2I}$	
Superposition	(1,1,1,1) 4		$\frac{ 0\rangle + 1\rangle}{\sqrt{2}} \otimes \frac{ 0\rangle + 1\rangle}{\sqrt{2}} \otimes 00\rangle$ $\xrightarrow{U_F}$	
Entanglement	(1,1,1,1) 4		$\frac{1}{2} \left(00\rangle \otimes 00\rangle + 01\rangle \otimes 01\rangle - 10\rangle \otimes 10\rangle - 11\rangle \otimes 11\rangle \right)$ $\xrightarrow{QFT_2 \otimes I}$	
Interference	(1,0,1,0) 2		$\frac{1}{4} \left(0000\rangle - 0001\rangle + 0010\rangle - 0011\rangle + 0100\rangle - 0101\rangle + 0110\rangle - 0111\rangle \right)$	

From Table 17 the following is observed:

- The entanglement operator creates very strong quantum correlation among vectors 1, 2, 3 and 4. This correlation identifies the input function that has the maximal period (and so maximal entanglement).

- The entanglement operator creates the quantum correlation with negative conditional entropies between qubits 1 and 2, and between qubits 3 and 4. This is the nonclassical supercorrelation effect from entanglement operator.
- The interference operator preserves quantum correlation, but does not decrease the classical entropy because entanglement is too great (degree of resistance is very high).

Shor's algorithm undergoes the special structure of its input space: periodical functions. Every function is characterized by its capacity to create quantum entanglement, which depends on its period. In Fig. 3 this structure is pictured.

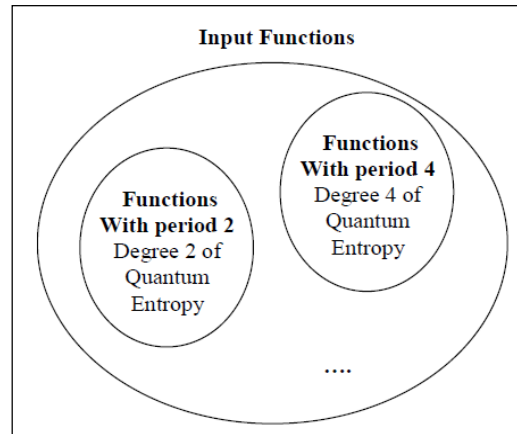


Figure 3. Quantum Information Structure of Shor's Input Space

Physical interpretation of the analysis results

1	When the QA computation begins, the Shannon entropy coincides with the von Neumann entropy, but they are both zero. The intelligence is then maximal since the system is in a basis state.
2	The superposition operator increases the Shannon entropy of the first n qubits to its maximum, but leaves the von Neumann entropy unchanged. The intelligence is minimal since the degree of disorder is at its maximum but has not been stored into the system yet.
3	The entanglement operator increase the von Neumann entropy of the first n qubits according to f , but leaves the Shannon entropy unchanged. The intelligence increase at this step since some information is stored into quantum correlation using super-correlation that created by the present of a new effect in evolution of QA's as the negative conditional entropy between the partial qubits
4	4.1. The interference operator preserves quantum correlation, but transpose it between basis vectors; this transposing maintains the period of the input function encoded, but it has as side effect to reduce the classical entropy, letting possible to access the period information generating an intelligent state, namely a state containing all required quantum information but with minimum classical entropy as a qualitative measure of free energy.
	4.2. The interference operator does not change the value of the von Neumann entropy introduced by the entanglement operator, but decreases the value of the Shannon entropy to its minimum, that is to the value of the von Neumann entropy itself. The intelligence of the state reaches its maximum again, but now with a non-zero quantity of information in quantum correlation.

As described above, the von Neumann entropy can be interpreted as the degree of information in a vector, namely, as a measure of the information stored in quantum correlation about the function f . The Shannon entropy is interpreted as the measure of the degree of inaccessibility of this information through the meas-

urement. In this context, the QG G of Eq. (39) transfers information from f into the output vector minimizing the quantity of unnecessary noise producible by the measurement, or, more technically, minimizing the non-negative, according to

$$S_T^{Sh}(|output\rangle) - S_T^{vN}(|output\rangle) = \Delta S(|output\rangle)$$

(the defect exchange of measurement entropy) with $T = \{1, \dots, n\}$. The intelligence of the output state increases while the average unnecessary noise decreases. According to this definition, the action of the QFT in the Shor's algorithm is to associate with every possible function f a maximally intelligent output state, namely a state $|output\rangle$ such that $\mathcal{J}_T(|output\rangle) = 1$. This is clear from the graphical representation of the information flow and the intelligence relative to the two functions considered in Example in Fig. 4. If the period r does not divide 2^n exactly, then the QFT is not optimal. In fact the final superposition for the first n qubits is not a periodical superposition. Nevertheless, by increasing the number n of qubits used for encoding input strings, it is possible to approximate this periodical superposition as well as desired.

The way the function f is encoded into the operator U_F and the set T used for the calculation of the QA-intelligence $\mathcal{J}_T(|output\rangle)$ are problem dependent.

Consider, for instance, the Deutsch-Jozsa decision making QA problem: one must decide if a Boolean function $f : \{0,1\}^n \rightarrow \{0,1\}$ is constant or balanced.

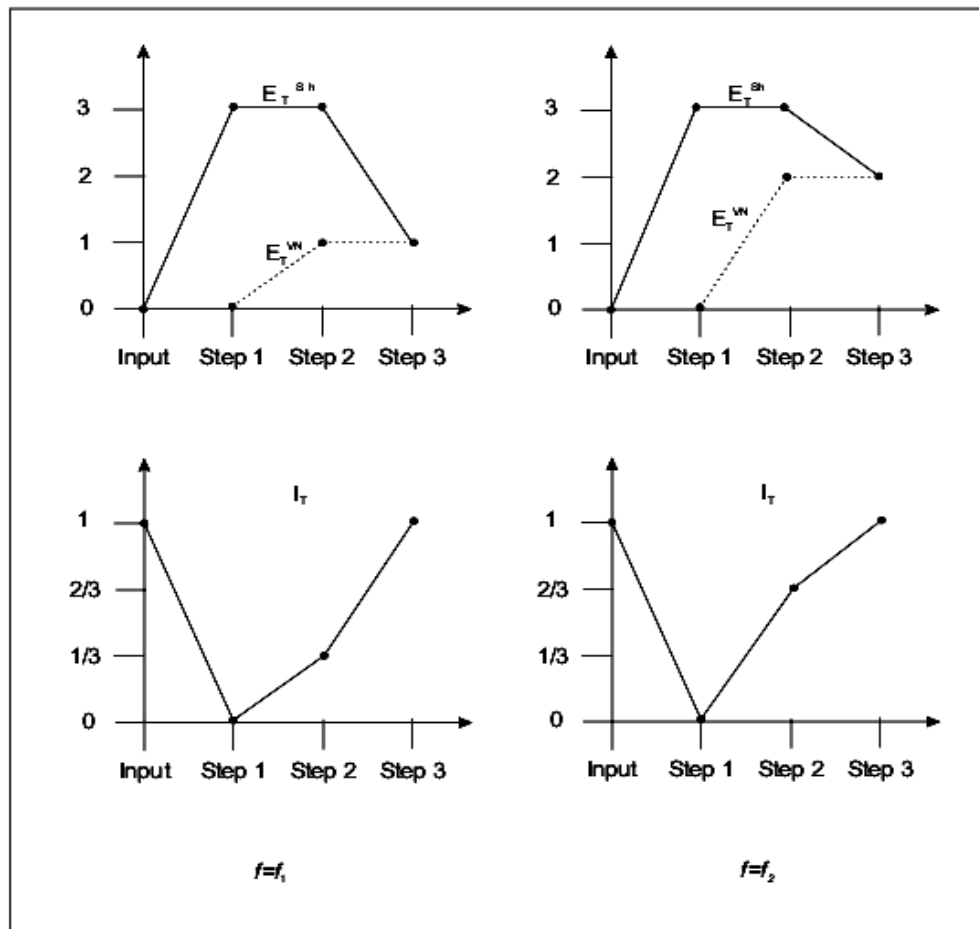


Figure 4. Information flow and intelligence of the Shor's QA

The same encoding scheme of the Shor's algorithm can be used to solve this problem. In this case, after the entanglement operator has acted, the von Neumann entropy of every proper subset of the first n qubits is always 0, whereas the von Neumann entropy of the first n qubits is 1 for some balanced functions. This

means that for these functions no interference operator in the form $Int \otimes I_m$ can increase the intelligence of the state with respect to the first n qubits, as it happens in the Shor's algorithm.

In other words, the state of the system after entanglement has been applied is already maximally intelligent with respect to first n qubits and the information accessibility cannot be increased through the application of any interference operator. One solution to this problem is to encode f into the unitary operator $U_F \cdot [I_n \otimes (H \cdot C)]$ where U_F is obtained as in the Shor's algorithm.

With this encoding scheme, the von Neumann entropy of the first n qubits after Step 2 is always 0. On the contrary, the von Neumann entropy of any subset of the first n qubits can be positive, implying entanglement between this subset and the rest of the system. In particular, every singleton constituted by one qubit may be characterized by a positive value of the von Neumann entropy. The Deutsch-Jozsa QA interference operator is chosen in order to reduce as much as possible the gap between the Shannon and the von Neumann entropies of every one of these singletons.

This operator is the Walsh-Hadamard transform of order n , defined as the tensor power H_n . Indeed, it is easy to verify that for every state $|\psi\rangle$ and every qubit i , the matrix $(H^{-1} \cdot |\psi\rangle\langle\psi|_{\{i\}} \cdot H)$ is diagonal. This means the action of H_n is to maximize the intelligence of every one of the first n qubits by annihilating the gap between its Shannon and von Neumann entropies.

Information-theoretical analysis of Grover's quantum search algorithm

The searching problem can be stated in terms of a list $\mathcal{L}[0,1,...,N-1]$ with a number N of unsorted elements. Denote by x_0 the marked element in \mathcal{L} that are sought. The quantum mechanical solution of this searching problem goes through the preparation of a quantum register in a quantum computer to store the N items of the list. This will allow exploiting quantum parallelism. Thus, assume that the quantum registers are made of n source qubits so that $N = 2^n$.

A target qubit is used to store the output of function evaluations or calls.

To implement the quantum search, construct a unitary operation that discriminates between the marked item x_0 and the rest. The following function

$$f_{x_0}(x) = \begin{cases} 0, & \text{if } x \neq x_0 \\ 1, & \text{if } x = x_0 \end{cases},$$

and its corresponding unitary operation $U_{f_{x_0}} |x\rangle|y\rangle = |x\rangle|y \oplus f_{x_0}(x)\rangle$. Count how many applications of this operation or oracle calls are needed to find the item. The rationale behind the Grover algorithm is: 1) to start with a quantum register in a state where all the computational basis states are equally present; 2) to apply several unitary transformations to produce an outcome state in which the probability of catching the marked state $|x_0\rangle$ is large enough.

The steps in Grover's algorithm are shown in tabular form below.

Step	Computational algorithm	Formula
Step 1	Initialize the quantum registers to the state: $ \psi_1 = input\rangle := 00...0\rangle 1\rangle$.	(62)
Step 2	Apply bit-wise the Hadamard one-qubit gate to the source register, so as to produce a uniform superposition of basis states in the source register, and also to the target register: $ \psi_2\rangle := U_H^{\otimes(n+1)} \psi_1\rangle = \frac{1}{2^{(n+1)/2}} \sum_{x=0}^{2^n-1} x\rangle \left[\sum_{y=0,1} (-1)^y y\rangle \right].$	(63)
Step 3	Apply the operator $U_{f_{x_0}}$: $ \psi_3\rangle := U_{f_{x_0}} \psi_2\rangle = \frac{1}{2^{(n+1)/2}} \sum_{x=0}^{2^n-1} (-1)^{f_{x_0}(x)} x\rangle \left[\sum_{y=0,1} (-1)^y y\rangle \right].$ Let U_{x_0} be the operator by $U_{x_0} x\rangle := (1 - 2 x_0\rangle\langle x_0) x\rangle = \begin{cases} - x_0\rangle & \text{if } x = x_0 \\ x\rangle & \text{if } x \neq x_0 \end{cases},$ that is, it flips the amplitude of the marked state leaving the remaining source basis states unchanged. The state in the source register of Step 3 equals precisely the result of the action of U_{x_0} , i.e., $ \psi_3\rangle = ([1 - 2 x_0\rangle\langle x_0] \otimes I) \psi_2\rangle.$	(64)
Step 4	Apply next the operation D known as inversion about the average. This operator is defined as follows $D := -(U_H^{\otimes n} \otimes I) U_{f_0} (U_H^{\otimes n} \otimes I)$, and $ \text{output}\rangle = D \psi_3\rangle$, where U_{f_0} is the operator in Step 3 for $x_0 = 0$. The effect of this operator on the source is to transform $\sum_x \alpha_x x\rangle \mapsto \sum_x (-\alpha_x + \langle \alpha \rangle) x\rangle$, where $\langle \alpha \rangle := 2^{-n} \sum_x \alpha_x$ is the mean of the amplitudes, so its net effect is to amplify the amplitude of $ x_0\rangle$ over the rest.	(65)
Step 5	Iterate Steps 3 and 4 a number of times m .	
Step 6	Measure the source qubits (in the computational basis). The number m is determined such that the probability of finding the searched item x_0 is maximal.	

According to Steps 2 – 4 above, the QAG of Grover's quantum search algorithm (QSA) is

$$G = (D_n \otimes I) \cdot U_F \cdot ({}^n H \otimes H)$$

that acts on the initial state of both registers in the QSA.

Computational analysis of Grover's QSA is similar to analysis of the Deutsch-Jozsa QA. The basic component of the algorithm is the quantum operation encoded in Steps 3 and 4, which is repeatedly applied to the uniform state $|\psi_2\rangle$ in order to find the marked element. Steps 5 and 6 in Grover's algorithm are also applied in Shor's QSA. Although this procedure resembles the classical strategy, Grover's operation enhances by constructive interference of quantum amplitudes (see Table 16) the presence of the marked state.

The operator encoding the input function is

$$U_F = \begin{pmatrix} I & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & C & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & I & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & I & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & I & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & I & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & I \end{pmatrix}. \quad (66)$$

Table 18 represents a general iteration algorithm for information analysis of Grover's QSA according to the above presented algorithm.

Table 18. Information Analysis of Grover's Algorithm (General Iteration)

Step	Classical and Quantum Entropy $S_{ \psi\rangle}(\{j\}) = -\lambda_1 \log \lambda_1 - \lambda_2 \log \lambda_2$	States and Gate Operations
Input	$\lambda_{1,2} = \frac{\alpha^2}{2} \left(-1 + 2^n + \frac{\beta^2}{\alpha^2} \pm \sqrt{5 - 2^{n-2} + 2^{2n} + (2^{n-2} - 8) \frac{\beta}{\alpha} + 2 \frac{\beta^2}{\alpha^2} + \frac{\beta^4}{\alpha^4}} \right)$ $H_{sh}(\psi\rangle) = -(2^n - 1) \alpha^2 \log \alpha^2 - \beta^2 \log \beta^2$	$\alpha \left(0\dots 0\rangle - \dots - \frac{\beta}{\alpha} x\rangle - \dots - 1\dots 1\rangle \right) \otimes \frac{ 0\rangle - 1\rangle}{\sqrt{2}}$
Entangle-ment	$\lambda_{1,2} = \frac{\alpha^2}{2} \left(-1 + 2^n + \frac{\beta^2}{\alpha^2} \pm \sqrt{5 - 2^{n-2} + 2^{2n} - (2^{n-2} - 8) \frac{\beta}{\alpha} + 2 \frac{\beta^2}{\alpha^2} + \frac{\beta^4}{\alpha^4}} \right)$ $H_{sh}(\psi\rangle) = -(2^n - 1) \alpha^2 \log \alpha^2 - \beta^2 \log \beta^2$	$\alpha \left(0\dots 0\rangle + \dots - \frac{\beta}{\alpha} x\rangle + \dots + 1\dots 1\rangle \right) \otimes \frac{ 0\rangle - 1\rangle}{\sqrt{2}}$
Interference	$\lambda_{1,2} = \frac{(\alpha - m)^2}{2} \left(-1 + 2^n + \frac{(\beta + m)^2}{(\alpha - m)^2} \pm \sqrt{5 - 2^{n-2} + 2^{2n} - (2^{n-2} - 8) \frac{\beta + m}{\alpha - m} + 2 \left(\frac{\beta + m}{\alpha - m} \right)^2 + \frac{(\beta + m)^4}{(\alpha - m)^4}} \right)$ $H_{sh}(\psi\rangle) = -(2^n - 1) (\alpha - m)^2 \log (\alpha - m)^2 - (\beta + m)^2 \log (\beta + m)^2$	$(\alpha - m) \left(0\dots 0\rangle + \dots + \frac{\beta - m}{\alpha - m} x\rangle - \dots - 1\dots 1\rangle \right) \otimes \frac{ 0\rangle - 1\rangle}{\sqrt{2}}$

Tables 19 and 20 two iterations of this algorithm with the operator U_F from Eq. (66) are reported.

From these tables, the following are observed:

1	The entanglement operator in each iteration increase correlation among the different qubits.
2	Super-correlation from entanglement operator is created according to negative conditional entropies between different qubits.
3	Interference operator reduces the classical Shannon entropy but it destroys part of the quantum super-correlation measure by conditional and von Neumann entropy.

Table 19. Information Analysis of Grover's Algorithm (First Iteration)

Step	Classical Entropy $H_{sh}(\{\psi\})$	Quantum Entropy $S_{\psi}(\{j\})$	States and Gate Operations	Dynamics of Solution Probabilities
Input	0		$ 000\rangle \otimes 1\rangle$ $\downarrow [H]$	
Superposition	4		$\frac{ 0\rangle+ 1\rangle}{\sqrt{2}} \otimes \frac{ 0\rangle+ 1\rangle}{\sqrt{2}} \otimes \frac{ 0\rangle+ 1\rangle}{\sqrt{2}} \otimes \frac{ 0\rangle- 1\rangle}{\sqrt{2}}$ $\downarrow [U_F]$	
Entanglement	4	$L = 2 - \frac{3}{4} \log 3$	$\frac{1}{2\sqrt{2}} \left(\begin{matrix} 000\rangle & 001\rangle & 010\rangle \\ 011\rangle & - 100\rangle & 101\rangle \\ + 110\rangle & + 111\rangle \end{matrix} \right) \otimes \frac{ 0\rangle- 1\rangle}{\sqrt{2}}$ $\downarrow [D_3 \otimes I]$	
Interference	$5 - \frac{25}{16} \log 5$	$L = -\frac{1}{8} (4 - \sqrt{13}) \log \left[\frac{1}{8} (4 - \sqrt{13}) \right] - \frac{1}{8} (4 + \sqrt{13}) \log \left[\frac{1}{8} (4 + \sqrt{13}) \right]$	$\frac{1}{4\sqrt{2}} \left(\begin{matrix} 000\rangle - 5 001\rangle - 010\rangle \\ 011\rangle - 100\rangle + 101\rangle \\ + 110\rangle + 111\rangle \end{matrix} \right) \otimes \frac{ 0\rangle- 1\rangle}{\sqrt{2}}$	

Grover's QSA builds in several iterations any intelligent states. Since each iteration encodes the searched function by entanglement, but then partly destroys the encoded information by the interference operator, several iterations are needed in order to conceal both the need to have encoded information and the need to access it.

Methodologically, the principle of maximal intelligence on output states is used for synthesizing QAGs. In general, the joint action of the superposition operator and of entanglement operator is to introduce the information necessary to solve the problem in the system quantum correlation.

This information, measured through the von Neumann entropy of every qubit, cannot explode, since this would mean too much randomness in the final outcome. The interference operator must reduce the randomness of the output state as much as possible. This means the interference operator is chosen in such that it preserves the von Neumann entropy, but makes the Shannon entropy collapse on its lower bound.

Table 20. Information Analysis of Grover's Algorithm (Second Iteration)

Step	Classical Entropy $H_{sh}(\{\psi\})$	Quantum Entropy $S_{\psi}(\{j\})$	States and Gate Operations	Dynamics of Solution Probabilities
Entanglement	$5 - \frac{25}{16} \log 5$	$L = -\frac{1}{16} (8 - \sqrt{37}) \log \left[\frac{1}{16} (8 - \sqrt{37}) \right] - \frac{1}{16} (8 + \sqrt{37}) \log \left[\frac{1}{16} (8 + \sqrt{37}) \right]$	$\downarrow [U_F]$ $\frac{1}{4\sqrt{2}} \left(\begin{matrix} 000\rangle - 5 001\rangle + 010\rangle \\ 011\rangle + 100\rangle - 101\rangle \\ + 110\rangle + 111\rangle \end{matrix} \right) \otimes \frac{ 0\rangle- 1\rangle}{\sqrt{2}}$ $\downarrow [D_3 \otimes I]$	
Interference	$6 - \frac{121}{64} \log 11$	$L = -\frac{1}{256} (128 - \sqrt{14656}) \log \left[\frac{1}{256} (128 - \sqrt{14656}) \right] - \frac{1}{256} (128 + \sqrt{14656}) \log \left[\frac{1}{256} (128 + \sqrt{14656}) \right]$	$-\frac{1}{8\sqrt{2}} \left(\begin{matrix} 000\rangle - 11 001\rangle + 010\rangle \\ 011\rangle + 100\rangle + 101\rangle \\ + 110\rangle + 111\rangle \end{matrix} \right) \otimes \frac{ 0\rangle- 1\rangle}{\sqrt{2}}$	

From the application standpoint, the existence of a measure for the intelligence degree of a state allows the combination of QA techniques for encoding functions with some other computational methods, such as genetic algorithms. In this context, the measure of unnecessary noise becomes a fitness function in order to measure the desirability of a result. Thus, quantum computing provides a way of processing information that can be used in the classical problem solving domain.

Simulation results of QA-termination problem solution based on principle of Shannon/von Neumann minimum entropy

From the step-by-step majorization principle of QA's it follows that for efficient termination of QA's that give the highest probability of successful result, the Shannon entropy was minimal for the step $m+1$. This is the principle of minimum Shannon entropy for termination of a QA with the successful result. This result also follows from the principle of QA maximum intelligent state as in Eq. (0). For this case according to Eq. (0)

$$\begin{aligned} \max \mathcal{J}_T(|\psi\rangle) &= 1 - \min \frac{H_T^{Sh}(|\psi\rangle)}{|T|}, \\ S_T^{vN}(|\psi\rangle) &= 0 \quad (\text{for pure quantum state}) \end{aligned} \quad (67)$$

Thus, the principle of maximal intelligence of QA's include as particular case the principle of minimum Shannon entropy for QA-termination problem solution.

QA-termination problem solving based on minimum Shannon/von Neumann dynamic simulation entropy

Consider the complete basis vector

$$|A\rangle = a_1|0\dots 0\rangle + a_2|0\dots 1\rangle + \dots + a_{2^n}|1\dots 1\rangle.$$

For this case, the Shannon entropy is

$$S^{Sh}(|A\rangle) = -\sum_{i=1}^{2^n} a_i^2 \log a_i^2, \quad S^{vN}(|A\rangle) = -\sum_{i=1}^{2^n} \lambda_i(a_i^T a_i) \log \lambda_i(a_i^T a_i) \quad (68)$$

where $\lambda_i(a_i^T a_i)$ are eigenvalues of quantum state $|A\rangle$. Using the decomposition of quantum state vector $|A\rangle$ with the selection of measurement and calculation:

$$\begin{aligned} |A\rangle &= a_1|0\dots 0\rangle|0\rangle + a_2|0\dots 0\rangle|1\rangle + \dots + a_{2^{n-1}}|1\dots 1\rangle|0\rangle + a_{2^n}|1\dots 1\rangle|1\rangle \\ &= [a_1|0\dots 0\rangle + a_3|0\dots 1\rangle + \dots + a_{2^{n-1}}|1\dots 1\rangle]|0\rangle \\ &\quad + [a_2|0\dots 0\rangle + a_4|0\dots 1\rangle + \dots + a_{2^n}|1\dots 1\rangle]|1\rangle \end{aligned}$$

or

$$|A\rangle = |A\rangle_{|0\rangle} + |A\rangle_{|1\rangle}. \quad (69)$$

Then the partial entropy can be calculated as

$S_{ 0\rangle}^{Sh} = -\sum_i a_i^2 \log a_i^2$	$S_{ 0\rangle}^{vN} = -\sum_i \lambda_i(a_i^T a_i) \log \lambda_i(a_i^T a_i)$	(70)
$S_{ 1\rangle}^{Sh} = -\sum_{j \neq i} a_j^2 \log a_j^2$	$S_{ 1\rangle}^{vN} = -\sum_i \lambda_i(a_i^T a_i) \log \lambda_i(a_i^T a_i)$	

where $i=1,3,\dots,2^{n-1}$, $j=2,4,\dots,2^n$.

In the more general case of Shor's QA, $i = [i_0, i_0 + 2^n, \dots, 2^{2n} - i_0 + 1]$, where $i = 1$ for the state vector $|A\rangle_{|0\dots 0\rangle}$ and $i = 2^n$ for the state vector $|A\rangle_{|1\dots 1\rangle}$.

Fig. 5 shows the final simulation results of dynamic behavior for Shannon and von Neumann entropies according to Grover's operator (after 3 and 7 iterations) action (the case when intermediate results after superposition and entanglement applications are not shown).

Fig. 6 shows the simulation results of dynamic behavior for Shannon and von Neumann entropies according to superposition and entanglement operator (after 3 and 7 iterations) actions (the case when intermediate results after superposition and entanglement applications are shown).

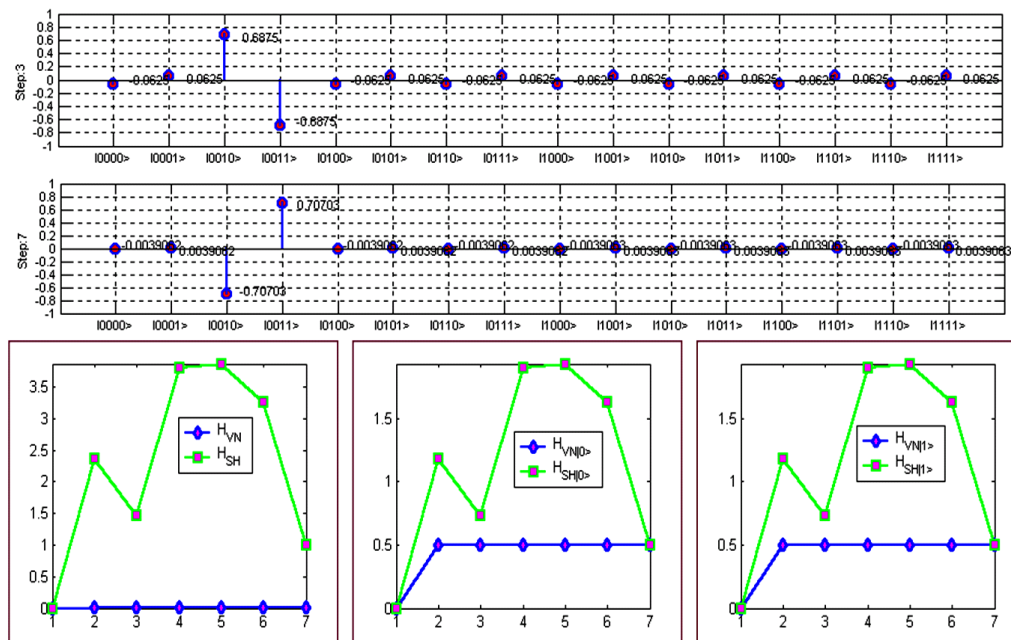


Figure 5. Simulation results of Grover algorithm (intermediate results after superposition and entanglement are not shown)

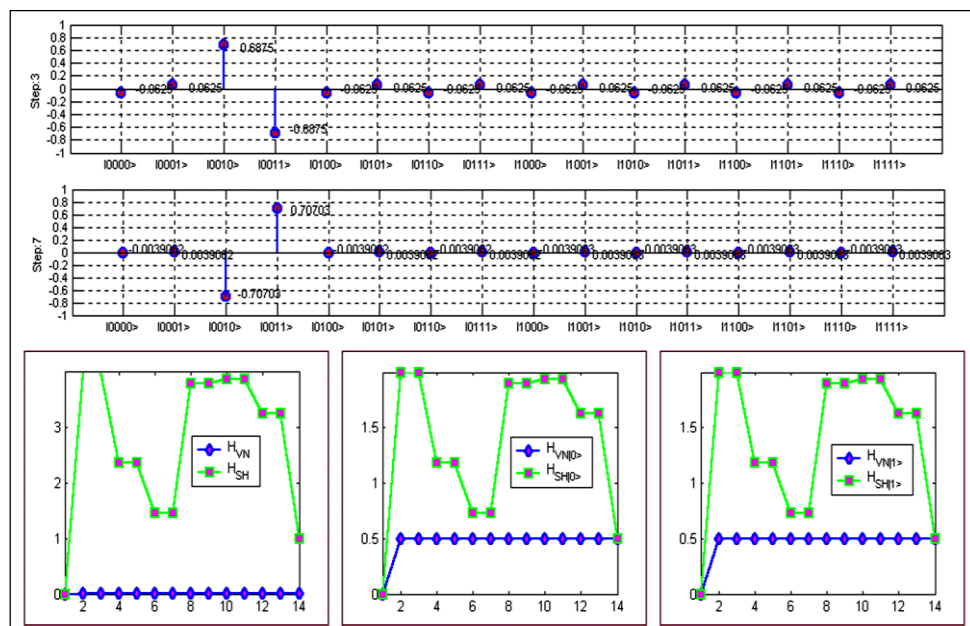


Figure 6. Simulation results of Grover algorithm (intermediate results after superposition and entanglement are shown)

Figs 5 and 6 show the action of constructive interference that created the maximal value 1 of intelligent state of Grover's QSA after 7 iterations.

Fig. 7 shows the final simulation results of dynamic behavior for Shannon and von Neumann entropies for Shor's QA (the case of 2 bit function – period 2) without intermediate simulation results after actions of superposition and entanglement operators.

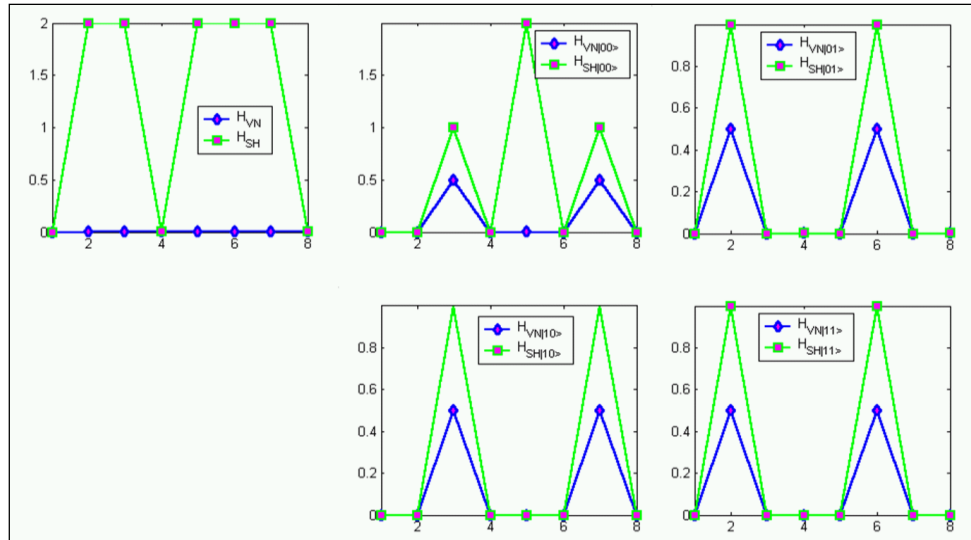


Figure 7. Simulation results of Shor algorithm

(intermediate results after superposition and entanglement are not shown, 2 bit function)

Fig. 8 shows the intermediate simulation results of dynamic behavior for Shannon and von Neumann entropies for Shor's QA (the case of 2 bit function – period 2) after actions of superposition and entanglement operators.

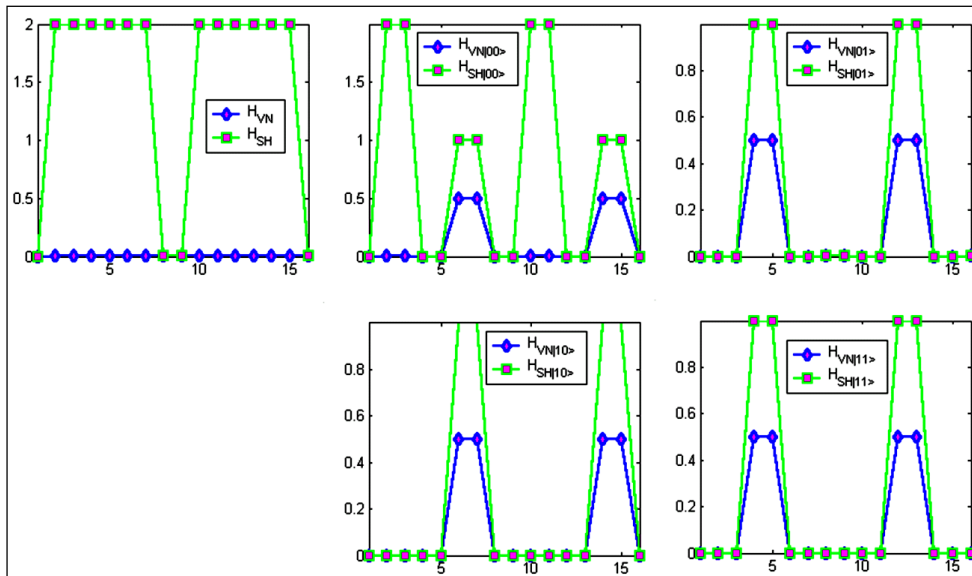
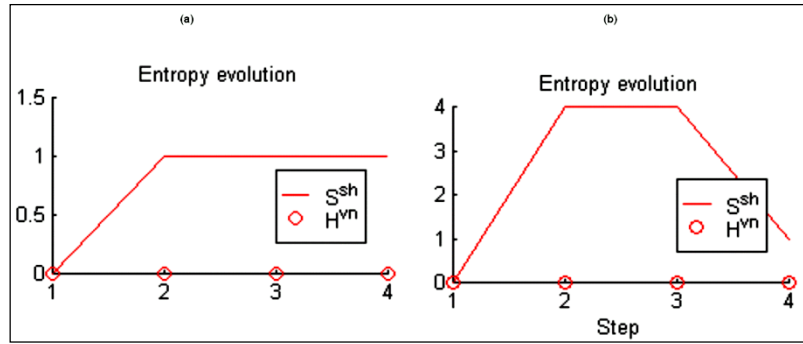


Figure 8. Simulation results of Shor algorithm

(intermediate results after superposition and entanglement are shown, 2 bit function (4 qubit))

Figs 7 and 8 show the action of constructive interference that created also as in Grover's QSA the maximal value 1 of intelligent state of Shor's QA after 14 iterations.

Figs 9 (a) – (d) show simulation results of dynamic behavior for Shannon and von Neumann entropies for termination of Deutsch, Deutsch-Jozsa, Grover's (with different search items number) and Shor's QAs respectively.



Figures 9 (a, b). Simulation results of dynamics behavior for Shannon and von Neumann entropies of Deutsch's and Deutsch-Jozsa's QA

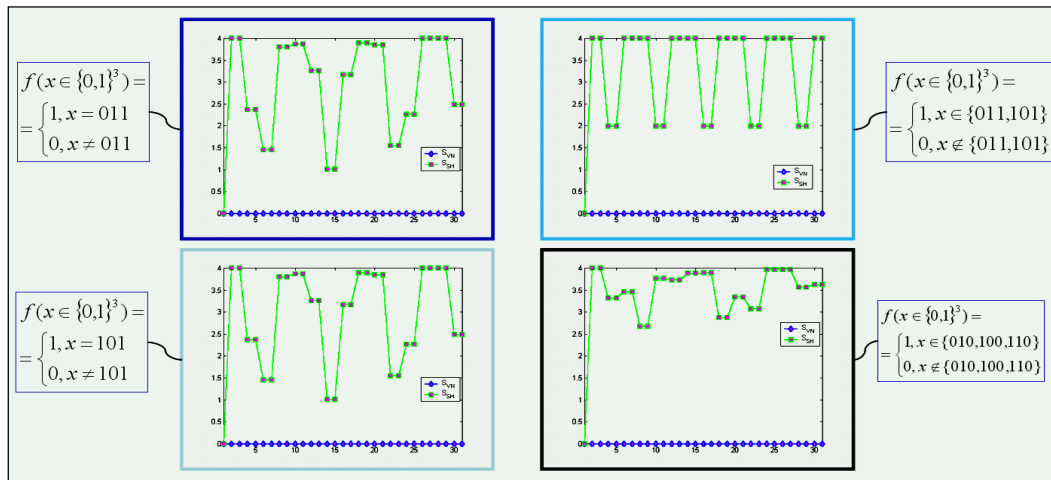


Figure 9 (c). Simulation results of dynamics behavior for Shannon and von Neumann entropies of Grover's QA

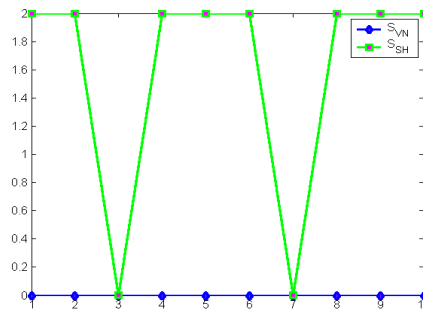


Figure 9 (d). Simulation results of dynamics behavior for Shannon and von Neumann entropies of Shor's QA

Analysis of QA-termination problem solving based on minimum Shannon/von Neumann dynamic simulation entropy

The diagonal matrix elements in Grover's QSA-operators are connected a database state to itself and the off-diagonal matrix elements are connected a database state to its neighbors 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.

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

where $a = 1 - b$.

If one of the states is marked, i.e. has its phase reserved with respect to those of the others, the multi-mode 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 $\frac{1}{N}[a + (N-1)b]^2$ for marked bit versus $\frac{1}{N}[a - (N-3)b]^2$ for the unmarked bits; N is the number of bits in the data register.

Grover algorithm is a optimal and it is very efficient search algorithm. And Grover-based software is currently used for search routines in large database.

Example. A quantitative measure of success in the database search problem is the reduction of the information entropy of the system following the search algorithm. Entropy $S^{Sh}(P_i)$ in this example of a single marked state is defined as

$$S^{Sh}(P_i) = -\sum_{i=1}^N P_i \log P_i, \quad (71)$$

where P_i is the probability that the marked bit resides in orbital i . In general, according to, 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,

$S(\rho_{(n-1)-mix}) = \log_2 N - 1 = S\left(\rho_{\left(\frac{1}{\log_2 N}\right)-pure}\right)$, 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 are used the Shannon information entropy for optimization of the termination problem of Grover's QSA. Information analysis of Grover's QSA based on using of Eq.(71), 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 $T \geq \left(\frac{1-P_e}{2\pi} + \frac{1}{\pi \log N}\right) \sqrt{N}$ times to

achieve a probability of error P_e . 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:

$$S_{init}^{Sh}(P_i) = -\log(1/N) = \log N.$$

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 orbitals may occasionally be detected by mistake. The entropy reduction can be calculated from the probability distribution, using Eq. (71).

Fig. 10 show the result of entropy calculation for the simulation quantum search of one marked state in the case $N = 7$.

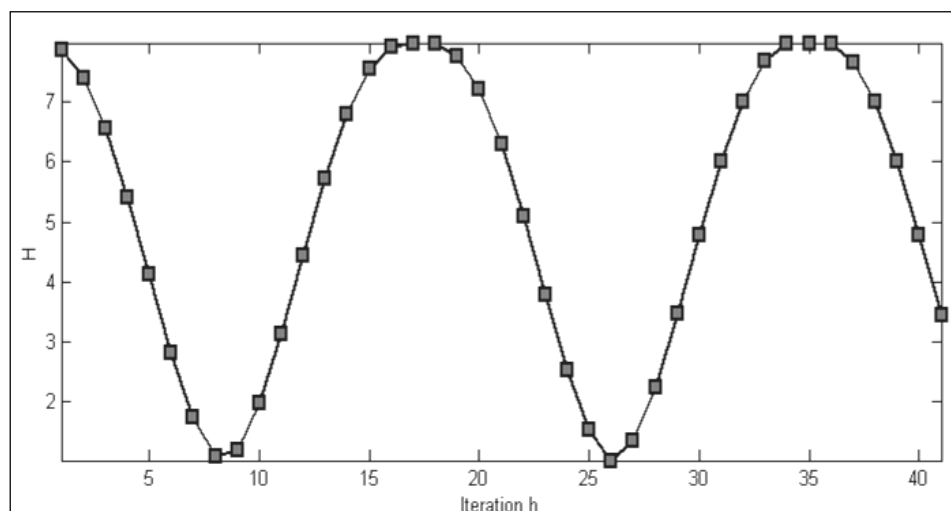


Figure 10. Shannon entropy analysis of Grover's QSA dynamics with seven inputs

References

1. Cerf N.J., Adami C. Negative entropy and information in quantum mechanics // *Physical Review Letters*. – 1997. – Vol. 79. – № 18. – Pp. 5195-5197.
2. Adami Ch. The physics of information // *Quantum Physics Archive* [http://arxiv.org/abs/arXiv: quant-ph/0405005v1](http://arxiv.org/abs/arXiv:quant-ph/0405005v1), 3 May 2004. – P. 28.
3. Adami Ch. Information theory in molecular biology // *Physics of Life Reviews*. – 2004. – Vol. 1. – № 1.
4. Horodecki M., Oppenheim J. and Winter A. Quantum information can be negative // *Quantum Physics Archive* [http://arxiv.org/abs/arXiv: quant-ph/0505062v1](http://arxiv.org/abs/arXiv:quant-ph/0505062v1), 9 May 2005. – P. 8.
5. Horodecki M., Oppenheim J., Winter A. Partial quantum information // *Nature*. – 2005. – Vol. 436. – № 7051.
6. Bose S., Rallan L. and Vedral V. Communication capacity of quantum computation // *Physical Review Letters*. – 2000. – Vol. 85. – № 25. – Pp. 5448-5451.
7. Nielsen M.A. and Chuang I.L. *Quantum Computation and Quantum Information*. – UK: Cambridge Univ. Press, 2000.
8. Ulyanov S.V., Litvintseva L.V., Ulyanov I.S., Ulyanov S.S. Quantum information and quantum computational intelligence: Quantum decision making and search algorithms // *Note del Polo Ricerca, Università degli Studi di Milano (Polo Didattico e di Ricerca di Crema)*. – Milan, 2005. – Vol. 84-85.
9. Ghisi F. and Ulyanov S.V. The information role of entanglement and interference in Shor quantum algorithm gate dynamics // *Journal of Modern Optics*. – 2000. – Vol. 47. – № 1 – Pp. 1012-1023.
10. Benenti G., Casati G., Strini G. *Principles of quantum computation and information*. – Singapore: World Scientific. – 2004. – Vol. I.; – 2007. – Vol. II.
11. Janzing D. *Computer science approach to quantum control* // *Habilitation: Univ. Karlsruhe (TH) Publ.* – Germany, 2006.
12. Ulyanov S.V., Litvintseva L.V., Ulyanov I.S. et al. Quantum information and quantum computational intelligence: Applied quantum soft computing in AI, computer science, quantum games and self-organization, informatics and design of intelligent wise robust control // *Note del Polo Ricerca*. – Milano: Università degli Studi di Milano Publ, 2007. Vol. 86.
13. Ingarden R.S. Quantum information theory // *Reports on Math. Physics*. – 1976. – Vol. 10. – № 1. – Pp. 43 – 79.

14. Ulyanov S.V. Generalized information measures and axiomatic information theory // Engineering Cybernetics (Science and Technics Investigations). – M.: VINITI Academy of Science USSR. – 1973. – Vol. 5. – Pp. 352-385.
15. Lomonaco S.L. Notes on quantum information theory. – Personal Lecture Notes. –Vol. 3. – URL: <http://www.cs.umbc.edu/~lomonaco/lecturenotes/index.html>.
16. Arian E. An information-theoretic analysis of Grover's algorithm // Quantum Physics Archive <http://arxiv.org/abs/arXiv: quant-ph/0210068>, 10 Oct 2002. – P. 9.
17. Ulyanov S.V., Kurawaki I., Yazenin A.V. et al. Information analysis of quantum gates for simulation of quantum algorithms on classical computers // Proceedings of Intern. Conf. on Quantum Communication, Measurements and Computing (QCM&C'2000). – Capri. Italy, 2000. Kluwer Acad. / Plenum Publ. – 2001. – Pp. 207-214.
18. Vedral V. The role of relative entropy in quantum information theory // Rev. Mod. Phys. 2000. – Vol. 74. – № 1. – Pp. 197-234.
19. Ulyanov S.V. System and method for control using quantum soft computing: US patent № 6,578,018B1. – 2003.
20. Ulyanov S.V., Litvintseva L.V., Ulyanov I.S. et al. Quantum information and quantum computational intelligence: Quantum probability, Physics of quantum information and Information geometry, Quantum computational logic and Quantum complexity // Note del Polo Ricerca. Milano: Universita degli Studi di Milano Publ. – 2007. – Vol. 83. – URL: available: <http://www.qcoptimizer.com>.