The information role of entanglement and interference operators in Shor quantum algorithm gate dynamics

F. GHISI†‡ and S. V. ULYANOV†‡

† Yamaha Motor Europe N. V. R&D Office
‡ Polo Didattico e di Ricerca di Crema – Milan University,
Via Bramante, 65 – 26013 CREMA(CR) – Italy

(*Received 28 October 1999; revision received 8 March 2000*)

Abstract. Shor algorithm dynamics of quantum computation states are analysed from the classical and the quantum information theory points of view. The Shannon entropy is interpreted 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 is defined. 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. We prove that the quantum Fourier transform 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 state.

1. Introduction

Most applications of quantum information theory have been developed in the domain of quantum communication systems, in particular in quantum source coding, quantum data compression [1, 2] and quantum error-correcting codes [3, 4]. Meanwhile quantum algorithms have been widely studied as computational processes [5–10]. In particular, much energy has been spent on the analysis of the Shor algorithm [5], which concerns the factorization of large integer numbers, attention being concentrated on its dynamics. In contrast, the information aspects involved in quantum computation have been developed analysing only the Toffoli gate [11].

In this paper, we investigate the possibility of using techniques from quantum information theory [11–13] in the domain of quantum algorithm synthesis and simulation. For this purpose, we analysed the classical and quantum information flow in the Shor algorithm. We show that the quantum gate G, which is 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 the classical Shannon entropy and the quantum von Neumann entropy. This principle is fairly general, suggesting both a methodology to design a quantum gate and a technique to efficiently simulate its behaviour on a classical computer.

Journal of Modern Optics ISSN 0950–0340 print/ISSN 1362–3044 online © 2000 Taylor & Francis Ltd
http://www.tandf.co.uk/journals

2. Computation dynamics of Shor quantum gate

In the Shor algorithm an integer number $n > 0$ and a function $f : \{0,1\}^n \rightarrow \{0,1\}^n$ are given such that f has 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 whith respect to its period. The problem is to find r. 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:

$$F(x,y) = (x, y \oplus f(x)) \tag{1}$$

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:

$$\tau(0) = |0\rangle \quad \tau(1) = |1\rangle \quad \tau(z_1 \cdots z_{2n}) = |z_1 \cdots z_{2n}\rangle \tag{2}$$

where $|0\rangle$ and $|1\rangle$ denote vectors $\begin{pmatrix}1\\0\end{pmatrix}$ and $\begin{pmatrix}0\\1\end{pmatrix}$, respectively, and $|z_1 \cdots z_{2n}\rangle$ stands for the tensor product $|z_1\rangle \otimes \cdots \otimes |z_{2n}\rangle$, being $z_1, \ldots, z_{2n} \in \{0,1\}$. We note that every bit value in a string is mapped into a vector of a Hilbert subspace of dimension 2. This subspace is called a qubit. Similarly, a sequence of successive bit values of length l is mapped into a vector of dimension 2^l. We call this subspace 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:

$$\forall z \in \{0,1\}^{2n} : U_F|z\rangle = |F(z)\rangle \tag{3}$$

Practically, the operator U_F is as follows:

$$[U_F]_{i,j} = \delta_{i,1+[F([j-1]_{(2)})]_{(10)}} \tag{4}$$

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 a unitary operator is not a peculiarity of the Shor algorithm, but it is typical of all known quantum algorithms [5, 9, 10]. In general, U_F contains the whole information about function f needed to solve the problem. In the Shor case, we could calculate the period r of f by testing the operator U_F on the input vectors $\underbrace{|0 \cdots 0\rangle}_{n} \otimes \underbrace{|0 \cdots 0\rangle}_{n}$ obtaining $\underbrace{|0 \cdots 0\rangle}_{n} \otimes \underbrace{|f(0 \cdots 0)\rangle}_{n}$, $\underbrace{|0 \cdots 1\rangle}_{n} \otimes \underbrace{|0 \cdots 0\rangle}_{n}$ obtaining $\underbrace{|0 \cdots 1\rangle}_{n} \otimes \underbrace{|f(0 \cdots 1)\rangle}_{n}$ and so on, until a vector $\underbrace{|x_1 \cdots x_n\rangle}_{n}$ for the first register of length n is found such that the corresponding vector $\underbrace{|f(x_1 \cdots x_n)\rangle}_{n}$ in the second register of length n coincides with $\underbrace{|f(0 \cdots 0)\rangle}_{n}$. The period r of f coincides with the binary number $x_1 \cdots x_n$. 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 time complexity of this algorithm is exponential for the worst case. In order to extract the information stored in U_F more efficiently, we must change our perspective. The operator U_F must in fact be used in order to transfer as much information as possible from the operator to the input vector each time U_F works. To this purpose, it is embedded into another unitary operator G, called the *quantum gate*, having the following general form:

$$G = (IF \otimes I_m) \cdot U_F \cdot (IF \otimes I_m) \tag{5}$$

where IF stands for a unitary squared matrix of order 2^n and I_m for the identity matrix of order 2^m. In the case of the Shor algorithm, U_F is embedded into the unitary quantum gate

$$G = (QFT_n \otimes I_n) \cdot U_F \cdot (QFT_n \otimes I_n) \tag{6}$$

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

$$[QFT_n]_{ij} = \frac{1}{2^{n/2}} \exp\left(2\pi J[(i-1)(j-1)/2^n]\right) \tag{7}$$

where J is the imaginary unit. The gate G does not act on many different basis input vectors any more. On the contrary it always gets as input the starting vector $\underbrace{|0 \cdots 0\rangle}_{n} \otimes \underbrace{|0 \cdots 0\rangle}_{n}$.

The corresponding computation evolves according to the following steps:

$$\text{Step 0} : |input\rangle = \underbrace{|0 \cdots 0\rangle}_{n} \otimes \underbrace{|0 \cdots 0\rangle}_{n} \tag{8}$$

$$\text{Step 1} : |\psi_1\rangle = (QFT_n \otimes I_n)|input\rangle = \frac{1}{2^{n/2}} \sum_{i_1, \ldots, i_n} |i_1 \cdots i_n\rangle \otimes |\underbrace{0 \cdots 0}_{n}\rangle \tag{9}$$

$$\text{Step 2} : |\psi_2\rangle = U_F|\psi_1\rangle = \frac{1}{2^{n/2}} \sum_{i_1, \ldots, i_n} |i_1 \cdots i_n\rangle \otimes |f(i_1 \cdots i_n)\rangle \tag{10}$$

$$\begin{aligned} \text{Step 3} : |output\rangle &= (QFT_n \otimes I_n)|\psi_2\rangle \\ &= \frac{1}{2^{n/2}} \sum_{\substack{j_1, \ldots, j_n \\ i_1, \ldots, i_n}} a_{i_1 \cdots i_n}^{j_1 \cdots j_n} |j_1 \cdots j_n\rangle \otimes |f(i_1 \cdots i_n)\rangle \end{aligned} \tag{11}$$

where

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

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

$$|output\rangle = \frac{1}{r} \sum_{p=0}^{r-1} \sum_{s=0}^{r-1} \exp\left(2\pi J s [i_1 \cdots i_n]_{(10)} l_p / r\right) |[s 2^n / r]_{(2)}\rangle \otimes |[p]_{(2)}\rangle \tag{12}$$

where l_p is an integer positive number and binary representations 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 quantum register. By repeating the algorithm a number of times polynomial in n and by performing a measurement each time, we can reconstruct the value of r [5].

In Step 1 the operator $QFT_n \otimes I_n$ acts on a basis vector. It transforms the vector source $|0 \cdots 0\rangle \otimes |0 \cdots 0\rangle$ into a linear combination of equally weighted basis vectors of the form $|i_1 \cdots i_n\rangle \otimes |0 \cdots 0\rangle$. Since every basis vector is interpreted as a possible observable state of the system, we say that QFT_n plays the role of the *superposition operator* for the first n qubits.

In Step 3 the operator $QFT_n \otimes I_n$ 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. probability amplitudes) 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 basis vectors. This summation can increase or decrease the resulting probability amplitudes. Since this phenomenon is very similar to classical wave interference, we say that in Step 3, the operator QFT_n plays the role of the *interference operator*. From the mathematical point of view, we observe that 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 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 non-local correlation among qubits. Therefore, we say U_F plays the role of the *entanglement operator*.

The quantum gates of the best-known quantum algorithms can all be described as the composition of a superposition, an entanglement and an interference operator, where the superposition and the interference operators always coincide, but play different roles, as it is 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.

Here we concentrate our attention on the action of these standard operators in the case of the Shor algorithm from the Information Theory viewpoint.

In order to illustrate the Shor algorithm, we propose two different computations in Example 1.

Example 1.

Let $n = 3$ and f_1, f_2 be defined as in table 1. Then

$$U_{F_1} = I_2 \otimes \begin{pmatrix} I_2 & 0 \\ 0 & C_2 \end{pmatrix} \otimes C \tag{13}$$

Table 1. 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

Table 2. Shor quantum gate information flow with $f = f_1$.

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

Table 3. Shor quantum gate state dynamics with $f = f_2$.

Step	State
Input	$\|000\rangle \otimes \|000\rangle$
Step 1	$\frac{\|0\rangle + \|1\rangle}{2^{1/2}} \otimes \frac{\|0\rangle + \|1\rangle}{2^{1/2}} \otimes \frac{\|0\rangle + \|1\rangle}{2^{1/2}} \otimes \|000\rangle$
Step 2	$\frac{\|0\rangle + \|1\rangle}{2^{1/2}} \otimes \frac{1}{2}(\|0000\rangle + \|0101\rangle + \|1010\rangle + \|1111\rangle) \otimes \|0\rangle$
Step 3	$\frac{1}{2}\left(\begin{array}{c} \|000\rangle \otimes \frac{\|0\rangle + \|1\rangle}{2^{1/2}} \otimes \frac{\|0\rangle + \|1\rangle}{2^{1/2}} + \|010\rangle \otimes \frac{\|0\rangle - \|1\rangle}{2^{1/2}} \otimes \frac{\|0\rangle - J\|1\rangle}{2^{1/2}} \\ + \|100\rangle \otimes \frac{\|0\rangle + \|1\rangle}{2^{1/2}} \otimes \frac{\|0\rangle - \|1\rangle}{2^{1/2}} + \|110\rangle \otimes \frac{\|0\rangle - \|1\rangle}{2^{1/2}} \otimes \frac{\|0\rangle - J\|1\rangle}{2^{1/2}} \end{array}\right) \otimes \|0\rangle$

and

$$U_{F_2} = I \otimes \begin{pmatrix} I_2 & 0 & 0 & 0 \\ 0 & I \otimes C & 0 & 0 \\ 0 & 0 & C \otimes I & 0 \\ 0 & 0 & 0 & C_2 \end{pmatrix} \otimes I \tag{14}$$

with

$$C = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{15}$$

The computation involved with these two operators is shown in table 2 and table 3.

3. 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

$$|\psi\rangle = \sum_{i_1\cdots,i_n\in\{0,1\}} c_{i_1\cdots i_n}|i_1\rangle\otimes|i_2\rangle\otimes\cdots\otimes|i_n\rangle \tag{16}$$

in a Hilbert space of dimension 2^n, let $T=\{j_1,\dots,j_k\}\subseteq\{1,\dots,n\}$ and $\{1,\dots,n\}-T=\{l_1,\dots,l_{n-k}\}$. We define

$$|\psi\rangle\langle\psi|_T = \sum_{\substack{t_{j_1},\dots,t_{j_k}\\ i_{j_1},\dots,i_{j_k}}} b^{t_{j_1}\cdots t_{j_k}}_{i_{j_1}\cdots i_{j_k}}|i_{j_1}\cdots i_{j_k}\rangle\langle t_{j_1}\cdots t_{j_k}| \tag{17}$$

where

$$b^{t_{j_1}\cdots t_{j_k}}_{i_{j_1}\cdots i_{j_k}} = \sum_{i_{l_1}=t_{l_1}\cdots\, i_{l_{n-k}}=t_{l_{n-k}}} c_{i_1\cdots i_n}c^*_{t_1\cdots t_n} \tag{18}$$

Choosing T means selecting a subspace of the Hilbert space of $|\psi\rangle$. If $T=\{j\}$, this subspace has dimension 2 and we call it the subspace of the qubit j. Similarly, if $T=\{j_1,\dots,j_k\}$, we say that we are dealing with the subspace of qubits $j_1,\dots,j_k$. $|\psi\rangle\langle\psi|_T$ describes the projection of the *density matrix* corresponding to $|\psi\rangle$ on this subspace.

We define the *Shannon entropy* of T in $|\psi\rangle$ with respect to the basis $B=\{|i_1\rangle\otimes\cdots\otimes|i_n\rangle\}$ as

$$E^{Sh}_T(|\psi\rangle) = -\sum_{i=1}^{2^k}[|\psi\rangle\langle\psi|_T]_{ii}\log_2[|\psi\rangle\langle\psi|_T]_{ii} \tag{19}$$

The Shannon entropy of T expresses the average information we gain when we measure the projection of $|\psi\rangle$ with respect to the projections of the vectors in B on the subspace of the qubits in T. The Shannon entropy can be interpreted as the degree of disorder involved with 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 also stores some other kind of information in non-local quantum 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 $|\psi\rangle$ we employ the *von Neumann entropy* of $|\psi\rangle$ with respect to T, which is defined as follows

$$E^{vN}_T(|\psi\rangle) = -\mathrm{tr}(|\psi\rangle\langle\psi|_T\log_2|\psi\rangle\langle\psi|_T) \tag{20}$$

where tr denotes the trace operator. 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 [12]. Note that we are dealing only with pure states and so the von Neumann entropy is a good measure of entanglement. In the case of mixed states, this would not be true and therefore our analysis can be applied only to ideal situations. However, we are dealing with the abstract form of quantum algorithms, without facing the problem of their implementation.

It is well known [16] that for every subset T

$$E^{Sh}_T(|\psi\rangle) \geq E^{vN}_T(|\psi\rangle) \tag{21}$$

Using these quantities, the *intelligence* $\Im_T(|\psi\rangle)$ of a state $|\psi\rangle$ with respect to the qubits in T and to the basis $B=\{|i_1\rangle\otimes\cdots\otimes|i_n\rangle\}$ is

$$\Im_T(|\psi\rangle) = 1-\frac{E^{Sh}_T(|\psi\rangle)-E^{vN}_T(|\psi\rangle)}{|T|} \tag{22}$$

From equation (21), by observing that for every vector $|\psi\rangle$ and every subset T then $E_T^{Sh}(|\psi\rangle) \leq |T|$, it is easy to show that

$$0 \leq \Im_T(|\psi\rangle) \leq 1 \tag{23}$$

The intelligence of a state with respect to T and B is minimal (i.e. 0) when $E_T^{vN}(|\psi\rangle) = 0$ and $E_T^{Sh}(|\psi\rangle) = |T|$, it is maximal (i.e.1) when $E_T^{vN}(|\psi\rangle) = E_T^{Sh}(|\psi\rangle)$.

4. Information analysis of the Shor quantum gate

How does the intelligence of $|\psi\rangle$ change while the Shor algorithm runs? We concentrate our attention on the set of the first n qubits, namely $T = \{1, \ldots, n\}$. We consider only the case where 2^n is a multiple of r.

The input vector defined in equation (8) is such that

$$E_T^{Sh}(|input\rangle) = E_T^{vN}(|input\rangle) = 0 \tag{24}$$

The intelligence of the state is:

$$\Im(|input\rangle) = 1 \tag{25}$$

Remark 1. Equation (24) is easily proved by observing that

$$|input\rangle\langle input|_T = |0\rangle\langle 0|_n \tag{26}$$

($|0\rangle\langle 0|_n$ is the nth 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 we conclude from equations (19) and (20) that the values of $E_T^{Sh}(|input\rangle)$ and $E_T^{vN}(|input\rangle)$ are both 0. In other words, the input state belongs to the measurement basis 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), the first n qubits undergo a unitary change of basis. This means their von Neumann entropy is left unchanged [16]. On the contrary, the Shannon entropy increases. From equation (19) we directly get the Shannon entropy value from the main diagonal values. This means that after Step 1 it is given by

$$E_T^{Sh}(|\psi_1\rangle) = n, \quad E_T^{vN}(|\psi_1\rangle) = 0 \tag{27}$$

The intelligence of the state with respect to the first n qubits is at this point

$$\Im_T(|\psi_1\rangle) = 0 \tag{28}$$

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 $k = 2^n/r$ an integer number, the state $|\psi_2\rangle$ can be written

$$|\psi_2\rangle = \sum_{l=0}^{r-1} (|[l]_{(2)}\rangle + |[l+r]_{(2)}\rangle + \cdots + |[l + (2^n/r - 1)r]_{(2)}\rangle) \otimes |f(l)\rangle \tag{29}$$

From equation (29), the densitity matrix $|\psi_2\rangle\langle\psi_2|_T$ is written as a $k \times k$ block matrix

$$|\psi_2\rangle\langle\psi_2|_T = \frac{1}{2^n}\begin{pmatrix} I(r) & I(r) & \cdots & I(r) \\ I(r) & I(r) & \cdots & I(r) \\ \cdots & \cdots & \cdots & \cdots \\ I(r) & I(r) & \cdots & I(r) \end{pmatrix} \tag{30}$$

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:

$$|\psi_2\rangle\langle\psi_2|_T = \frac{1}{2^{\log_2 k}}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}_{\log_2 k} \otimes \frac{1}{r}I(r) \tag{31}$$

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

$$E_T^{vN}(|\psi_2\rangle) = -(\log_2 k)\,\mathrm{tr}\left(\frac{1}{2}A\log_2\left(\frac{1}{2}A\right)\right) - \mathrm{tr}\left(\frac{1}{r}I(r)\log_2\left(\frac{1}{r}I(r)\right)\right) \tag{32}$$

with

$$A = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

Since $A/2$ is similar to $|1\rangle\langle 1|$ through a unitary change of basis, then equation (32) is written as

$$E_T^{vN}(|\psi_2\rangle) = -(\log_2 k)\,\mathrm{tr}\left(|1\rangle\langle 1|\log_2|1\rangle\langle 1|\right) - \mathrm{tr}\left(\frac{1}{r}I_r\log_2\left(\frac{1}{r}I_r\right)\right) = \log_2 r \tag{33}$$

We obtained the first equality in equation (33) by noting that $\mathrm{tr}(|1\rangle\langle 1|\log_2|1\rangle\langle 1|) = 0$. From the structure of the matrix in equation (30) we easily observe that the Shannon entropy did not change. Then, we conclude that for the set T of the first n qubits

$$E_T^{Sh}(|\psi_2\rangle) = n, \quad E_T^{vN}(|\psi_1\rangle) = \log_2 r \tag{34}$$

This means that

$$\Im_T(|\psi_2\rangle) = \frac{\log_2 r}{n} \tag{35}$$

Finally, when $QFT_n \otimes I_n$ is applied (Step 3), the last n qubits are left unchanged, whereas the first n qubits undergo a unitary change of basis through the quantum Fourier transform. This implies that the von Neumann entropy of the first n qubits is left unchanged. On the contrary, the Shannon entropy is reduced. Indeed, from equation (12), the output superposition of the first n qubits is periodic with period $k = 2^n/r$ and only r different basis vectors can be measured, every one with probability $1/r$. This means

$$E_T^{Sh}(|output\rangle) = \log_2 r, \quad E_T^{vN}(|output\rangle) = \log_2 r \tag{36}$$

The intelligence of the output state with respect to T is

$$\Im_T(|output\rangle) = 1 \tag{37}$$

Table 4. Shor quantum gate information flow with $f = f_1$.

Step	$E_T^{Sh}(\lvert\psi\rangle)$	$E_T^{VN}(\lvert\psi\rangle)$	$\Im_T(\lvert\psi\rangle)$
Input	0	0	1
Step 1	3	0	0
Step 2	3	1	1/3
Step 3	1	1	1

Table 5. Shor quantum gate information flow with $f = f_2$.

Step	$E_T^{Sh}(\lvert\psi\rangle)$	$E_T^{VN}(\lvert\psi\rangle)$	$\Im_T(\lvert\psi\rangle)$
Input	0	0	1
Step 1	3	0	0
Step 2	3	2	2/3
Step 3	2	2	1

From equation (37) it follows that the quantum Fourier transform preserves the von Neumann entropy and reduces the Shannon entropy of the first n qubits as much as possible.

The information analysis of two computations of the Shor algorithm is reported in Example 2.

Example 2. The two operators represented in table 1 produce the information flow reported in table 4 and table 5. It is worth observing how the intelligence of the state increases and decreases while the algorithm evolves.

5. Interpretation of the analysis results

From the above analysis we draw the following conclusions:

1. When the quantum algorithm computation begins the Shannon entropy coincides with the von Neumann entropy, but they are both zero. The intelligence is then maximal since we are dealing with 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 no information has been stored into the system yet.
3. The entanglement operator increases the von Neumann entropy of the first n qubits according to f, but leaves the Shannon entropy unchanged. The intelligence increases at this step since some information is stored into quantum correlation.
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. The intelligence of the state reaches its maximum again, but now with a non-zero quantity of information in quantum correlation.

The von Neumann entropy can be interpreted as the degree of informativity of a vector, 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 [12–14]. In this context, the quantum gate G of equation (6) 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 equation (21), quantity $E_T^{Sh}(|output\rangle) - E_T^{vN}(|output\rangle)$ with $T = \{1, \ldots, n\}$. The intelligence of an output state increases while the average unnecessary noise decreases. According to this definition, the action of the quantum Fourier transform in the Shor algorithm is to associate to every possible function f a maximally intelligent output state, namely a state $|output\rangle$ such that $\Im_T(|output\rangle) = 1$. This is clear from the graphical representation of the information flow and the intelligence relative to the two functions considered in example 1 (figure 1).

Remark 2. If the period r does not divide 2^n exactly, then the quantum Fourier transform 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 quibits used for encoding input strings, it is possible to approximate this periodical superposition as well as desired.

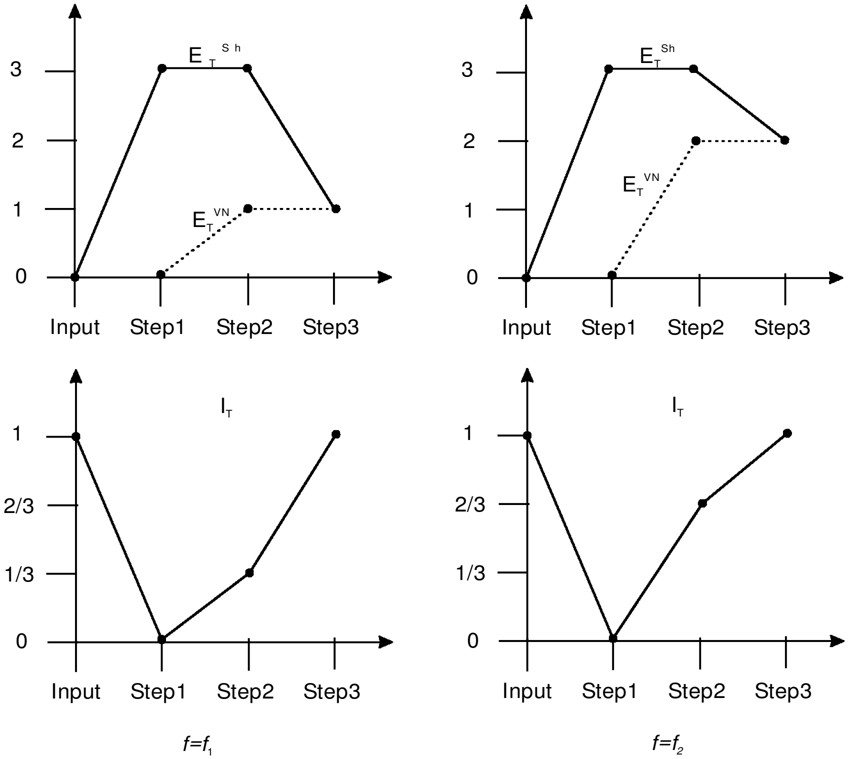

Figure 1. Information flow and intelligence of the Shor algorithm.

Remark 3. The way the function f is encoded into the operator U_F and the set T used for the calculation of the intelligence $\Im_T(|output\rangle)$ are problem dependent. Consider, for instance, the Deutsch–Jozsa decision problem [17]: one must decide if a Boolean function $f: \{0,1\}^n \to \{0,1\}$ is constant or balanced. We can use the same encoding scheme of the Shor algorithm to solve this problem. In this case we will observe that, 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 algorithm. In other words, the state of the system after the entanglement has been applied, is already maximally intelligent with respect to the 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 algorithm and H is defined as follows:

$$H = \frac{1}{2^{1/2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{38}$$

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 algorithm 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.

6. Conclusions and future developments

The analysis carried out looks interesting both from a methodological and an application point of view. Methodologically, the principle of maximal intelligence on output states can be assumed as a leading rule for synthesizing quantum gates. In general, the joint action of the superposition operator and of the entanglement operator is supposed to introduce the information necessary to solve the problem in the system quantum correlation. The interference operator must reduce the randomness of the output state, involved with the superposition operator, as much as possible. This means the interference operator is chosen in such a way that it preserves the von Neumann entropy, but makes the Shannon entropy collapse onto its lower bound, maximizing the intelligence of the output state.

From the application standpoint, the existence of a measure for the intelligence degree of a state suggests the possibility of combining quantum algorithm techniques for encoding functions with some other computational methods [15], such as genetic algorithms. In this context, the intelligence of a state becomes a sort of fitness function to measure the goodness of results. The leading idea is to look at quantum computing as a special way of processing information and to use its main features in the classical problem solving domain.

On the analysis level of quantum algorithms, the same information analysis carried on in this paper for the Shor algorithm should be done for other quantum algorithm benchmarks in order to have a global picture of the best-known quantum information processing techniques.

Acknowledgments

The authors are grateful to Professor Sandro Fornili and Professor Giovanni Degli Antoni for their valuable advice.

References

[1] Bennet, C., and Shor, P., 1998, *IEEE Trans. Inf. Theory*, **44,** 2724.
[2] Schumacher, B., 1995, *Phys. Rev. A*, **51,** 2738.
[3] Bennet, C., 1995, *Phys. Today*, **48,** 24.
[4] Cerf. N. J., and Cleve, R., 1997, *Phys. Rev. A*, **56,** 1721.
[5] Shor, P., 1997, *S.I.A.M. J. Computing*, **26,** 1484.
[6] Plenio, M. B., and Knight, P. L., 1996, *Phys. Rev. A*, **53,** 2986.
[7] Zalka, C., http://xxx.lanl.gov/ps/quant-ph/9806084.
[8] Ekert, A., and Jozsa, R., 1996, *Rev. Mod. Phys.*, **68,** 733.
[9] Simon, D. R., 1994, *Proc. 35th Annual IEEE Symposium on the Foundations of Computer Science* (IEEE Computer Society Press, Los Alamitos, CA), p. 124.
[10] Grover, L. K., 1996, *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing (STOC)*, p. 212.
[11] Ohya, M., and Watanabe, N., 1998, *Physica D*, **120,** 206.
[12] Cerf, N. J., and Adami, C., 1998, *Physica D*, **120,** 62.
[13] Ingarden, R. S., Kossakowski, A., and Ohia, M., 1997, *Information Dynamics and Open Systems* (Dordrecht: Kluiver Academic).
[14] Petrov, B., Goldenblat, I., and Ulyanov, S. V., 1982, *Advanced Control of Relativistic and Quantum Dynamic Systems: Information and Thermodynamics Aspects* (in Russian) (Moscow: Nauka).
[15] Cerf, N. J., and Koonin, S. E., 1998, *Math. Comput. Simulation*, **47,** 143.
[16] Preskill, J., 1997, http:://www.theory.caltech.edu/~presckill/ph229.
[17] Deutsch, D, and Jozsa, R., 1992, *Proc. R. Soc. London, Ser. A*, **439,** 553.