Found Phys (2009) 39: 559–572
DOI 10.1007/s10701-009-9302-0

The Algebraic Structure of an Approximately Universal System of Quantum Computational Gates

Maria Luisa Dalla Chiara · Roberto Giuntini · Hector Freytes · Antonio Ledda · Giuseppe Sergioli

Received: 17 February 2009 / Accepted: 17 March 2009 / Published online: 1 April 2009

Abstract Shi and Aharonov have shown that the Toffoli gate and the Hadamard gate give rise to an approximately universal set of quantum computational gates. We study the basic algebraic properties of this system by introducing the notion of Shi-Aharonov quantum computational structure. We show that the quotient of this structure is isomorphic to a structure based on a particular set of complex numbers (the closed disc with center $(\frac{1}{2}, \frac{1}{2})$ and radius $\frac{1}{2}$).

Keywords Quantum computation · Quantum logic

1 Introduction

Classical circuit theory is basically irreversible in the sense that Boolean functions (gates) are generally described as many-to-one: the same output-bits may correspond

Dedicated to Pekka Lahti.

M.L. Dalla Chiara
Dipartimento di Filosofia, Università di Firenze, via Bolognese 52, 50139 Firenze, Italy
e-mail: dallachiara@unifi.it

R. Giuntini (✉) · H. Freytes · A. Ledda · G. Sergioli
Dipartimento di Scienze Pedagogiche e Filosofiche, Università di Cagliari, via Is Mirrionis 1, 09123 Cagliari, Italy
e-mail: giuntini@unica.it

H. Freytes
e-mail: hfreytes@gmail.com

A. Ledda
e-mail: antonio.ledda@inwind.it

G. Sergioli
e-mail: giuseppe.sergioli@unisofia.it

to different input-bits. We know, however, that every Boolean gate has its own reversible counterpart, as shown by Toffoli [10]. The main idea is to consider the input-bits of a reversible gate as composed by two parts: a *control*-component which carries over the "actual" input-value and a *target*-component (*"ancilla"*), whose final value (after the application of the gate) represents the "actual" output. The price to pay is the increase of the computational space, due to the number of extra *ancilla*-bits needed to make the circuit reversible.

As is well known, the classical circuit-model of computation, both in its reversible and in its irreversible version, can be formulated by using a very small set of gates, called *universal set of gates*. This property (termed *functional universality*) amounts to saying that every gate can be mathematically simulated by means of a convenient composition of gates belonging to the universal set. For instance, in the irreversible case, the single gate NAND or the system consisting of the two gates AND and NOT turn out to be functionally universal. In the reversible case, such a role is played by a single gate: the *Toffoli gate* T (also called *controlled-controlled not*).

Unlike the classical circuit model, quantum computation "originates" in a naturally reversible way, because quantum gates are interpreted as unitary operators acting on pure states (*qubits* or *quregisters*) of the Hilbert space associated with the quantum circuit at issue. Being unitary, quantum gates represent reversible time-evolution of the circuit in question. Since there are uncountably many unitary operators, there is no hope to find any *finite* functionally universal set of quantum gates. The best we can do is having recourse to the notion of finite *approximate universality* [9]: a finite set of gates is said to be *approximately universal* iff any quantum gate can be approximated up to an arbitrary accuracy by a quantum circuit that consists of elements of this set.

Finding simpler and simpler sets of universal gates represents a crucial step in order to try and realize concrete quantum computers. Interestingly enough, this does not involve any serious loss in computational power; in fact, as proved by Solovay and Kitaev [8], shifting from a universal set to another one only causes a polylogarithmic overhead. The existence of a three-element (approximately) universal set of quantum gates has been proved by Deutsch in [6]. Many other universal sets were discovered afterwards, culminating in the result obtained by Shi [9] and further investigated by Aharonov [1]. These authors found a two-element universal set consisting of the (three-qubit) Toffoli gate T and of the one-qubit *Hadamard gate* $\sqrt{\mathtt{I}}$ (also called the *squareroot of the identity*). Unlike the classical reversible case, the Toffoli gate alone is not sufficient to reproduce the behavior of all quantum gates. A gate exhibiting a "genuine" quantum behavior needs to be added: a "good" example is represented by the operator $\sqrt{\mathtt{I}}$. From a foundational point of view, we can say that $\sqrt{\mathtt{I}}$ is just all that the Toffoli gate needs in order to reach quantum (approximate) universality, starting from classical (functional) universality.

The results we have mentioned so far are formulated in the framework of the usual approach to quantum computation, which is essentially based on quregisters and unitary operators of convenient Hilbert spaces. However, such a representation is unduly restrictive, since it does not encompass *open systems*, where interactions with an environment and some measurement-processes may occur. In this case, the time-evolution of quantum objects is no longer reversible. One can formulate a more

general model of quantum computational processes, where quregisters and unitary operators are replaced by density operators (*qumixes*) and by *unitary quantum operations*, respectively (see [2] and [7]).

From a physical point of view, using qumixes instead of quregisters has plenty of advantages. In fact, physical systems are never completely isolated and are always somehow interacting with the rest of the Universe. Hence, quantum states are better represented by qumixes (mixed states) instead of quregisters (pure states). Moreover (as shown by Aharonov, Kitaev and Nisan [2]), taking into account quantum circuits with qumixes allows us to treat some critical problems (such as measurements in the middle of a computation, decoherence, noise, and so on), which cannot be adequately represented in the framework of the usual approach. It should be noticed, however, that the Aharonov-Kitaev-Nisan model and the standard model are polynomially equivalent in computational power [2].

In this paper we will investigate some algebraic properties of the Shi-Aharonov universal set of gates (in their quantum operational form). To this aim we will equip the set of all qumixes with two quantum operations representing an appropriate generalization of the Toffoli gate $\mathtt{T}$ and of the Hadamard gate $\sqrt{\mathtt{I}}$.

We will show that the main algebraic properties of this structure can be also captured by restricting the action of the two quantum operations to qumixes "living" in the simplest Hilbert space, $\mathbb{C}^2$. In this way, the dimension of the Hilbert space associated with a reversible quantum circuit is dramatically reduced. The price to pay is the loss of the reversible nature of the two quantum operations.

2 Qubits, Quregisters and Qumixes

We will first sum up some basic concepts of quantum computation that will be used in the framework of our algebraic investigation. Consider the two-dimensional Hilbert space $\mathbb{C}^2$ (where any vector is represented by a pair of complex numbers). Let $\mathcal{B}^{(1)} = \{|0\rangle, |1\rangle\}$ be the canonical orthonormal basis for $\mathbb{C}^2$, where $|0\rangle = \binom{1}{0}$ and $|1\rangle = \binom{0}{1}$.

Definition 2.1 (Qubit) A *qubit* is a unit vector $|\psi\rangle = c_0|0\rangle + c_1|1\rangle$ of the Hilbert space $\mathbb{C}^2$.

The basis-elements $|0\rangle$ and $|1\rangle$ represent, in this framework, the two classical bits, which can be also interpreted as the classical truth-values *false* and *true*, respectively. Hence, from an intuitive point of view any qubit $|\psi\rangle = c_0|0\rangle + c_1|1\rangle$ can be regarded as a kind of "quantum perhaps": a superposition of the two classical truth-values, where the *Falsity* has probability $|c_0|^2$, while the *Truth* has probability $|c_1|^2$. From the physical point of view, a qubit describes the pure state of a single particle, while a system of n qubits (also called *n-quregister*) corresponds to the state of a compound system consisting of n particles. Accordingly, any n-quregister can be represented as a unit vector of the n-fold tensor product of the space $\mathbb{C}^2$:

$$\bigotimes^{n} \mathbb{C}^2 := \underbrace{\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_{n\text{-times}}$$

(where $\bigotimes^1 \mathbb{C}^2 := \mathbb{C}^2$). We will use $x, y, \ldots$ as variables ranging over the set $\{0, 1\}$, while $|x\rangle, |y\rangle, \ldots$ will range over the basis $\mathcal{B}^{(1)}$. Any factorized unit vector $|x_1\rangle \otimes \cdots \otimes |x_n\rangle$ of the space $\bigotimes^n \mathbb{C}^2$ will represent in this framework a *classical register* (a sequence of n bits). Instead of $|x_1\rangle \otimes \cdots \otimes |x_n\rangle$ we will also write $|x_1\rangle \ldots |x_n\rangle$ or, more briefly, $|x_1, \ldots, x_n\rangle$. Recall that the dimension of $\bigotimes^n \mathbb{C}^2$ is 2^n, while the set of all n-registers $\mathcal{B}^{(n)} = \{|x_1\rangle, \ldots, |x_n\rangle : x_i \in \{0, 1\}\}$ is an orthonormal basis for the space $\bigotimes^n \mathbb{C}^2$. We will call this set a *computational basis* for the n-quregisters. Since any string $x_1 \ldots x_n$ represents a natural number $j \in [0, 2^{n-1}]$ (where $j = 2^{n-1}x_1 + 2^{n-2}x_2 + \cdots + x_n$), any unit vector of $\bigotimes^n \mathbb{C}^2$ can be briefly expressed in the following form: $\sum_{j=0}^{2^{n-1}} c_j |j\rangle^{(n)}$, where $c_j \in \mathbb{C}$, $|j\rangle^{(n)}$ is the n-register corresponding to the number j and $\sum_{j=0}^{2^{n-1}} |c_j|^2 = 1$.

Quregisters are pure states; hence, from an intuitive point of view, they represent *maximal pieces of information*, that cannot be consistently extended to a richer knowledge. As mentioned in the Introduction, in quantum computation one cannot help referring also to non-maximal pieces of information; these correspond to *mixtures of quregisters* (also called *qumixes*), which are mathematically represented by density operators.

Definition 2.2 (Qumix) A *qumix* is a density operator of a Hilbert space $\bigotimes^n \mathbb{C}^2$.

We will indicate by $\mathfrak{D}(\bigotimes^n \mathbb{C}^2)$ the set of all qumixes of $\bigotimes^n \mathbb{C}^2$, while $\mathfrak{D} := \bigcup_{n=1}^{\infty} (\bigotimes^n \mathbb{C}^2)$ will denote the set of all possible qumixes.

Of course, quregisters can be described as special cases of qumixes.

The algebraic structure of the set $\mathfrak{D}$ of all qumixes essentially depends on the definition of a probability-function $\mathfrak{p}$ that assigns to any qumix ρ a probability-value. From an intuitive point of view, $\mathfrak{p}(\rho)$ represents the probability that the quantum information stored by ρ corresponds to a *true* information. In order to define the function $\mathfrak{p}$, we will first identify in any space $\bigotimes^n \mathbb{C}^2$ two special projections $P_0^{(n)}$ and $P_1^{(n)}$ that will represent the *Falsity* and the *Truth* properties, respectively. In this way, *Falsity* and *Truth* are dealt with as special cases of physical properties to which any density operator assigns a well determined probability-value, according to the quantum theoretic formalism.

Before defining $P_0^{(n)}$ and $P_1^{(n)}$, let us first distinguish two particular sets of natural numbers:

$$C_1^{(n)} := \left\{ i : |i\rangle^{(n)} = |x_1, \ldots, x_n\rangle \text{ and } x_n = 1 \right\};$$

$$C_0^{(n)} := \left\{ i : |i\rangle^{(n)} = |x_1, \ldots, x_n\rangle \text{ and } x_n = 0 \right\}.$$

On this basis, the *Falsity* and the *Truth* can be naturally defined as follows:

Definition 2.3 (Falsity and Truth)

(1) The *Falsity* of the space $\bigotimes^n \mathbb{C}^2$ is the projection $P_0^{(n)}$ onto the span of $\{|i\rangle^{(n)} : i \in C_0^{(n)}\}$ (the set of all *false registers*);

(2) The *Truth* of the space $\bigotimes^n \mathbb{C}^2$ is the projection $P_1^{(n)}$ onto the span of $\{|i\rangle^{(n)} : i \in C_1^{(n)}\}$ (the set of all *true registers*).

It turns out that for any $n > 1$:

$$P_1^{(n)} = I^{(r)} \otimes P_1^{(s)} \quad \text{and} \quad P_0^{(n)} = I^{(r)} \otimes P_0^{(s)}, \tag{2.1}$$

where $r + s = n$ and $I^{(r)}$ is the identity operator of $\bigotimes^r \mathbb{C}^2$.

Clearly, $P_1^{(n)} + P_0^{(n)} = I^{(n)}$. Furthermore, $P_1^{(n)}$ and $P_0^{(n)}$ are density operators if and only if $n = 1$.

Now, by applying the Born rule, the probability-function $\mathtt{p}$ can be defined as follows:

Definition 2.4 (Probability $\mathtt{p}$ of a qumix) For any qumix $\rho \in \mathfrak{D}(\bigotimes^n \mathbb{C}^2)$:

$$\mathtt{p}(\rho) := \mathtt{tr}\Big(P_1^{(n)}\rho\Big),$$

where $\mathtt{tr}$ is the trace-functional.

In other words, $\mathtt{tr}(\rho)$ represents the probability that the state ρ satisfies the Truth-property. In Sect. 4 we will see how the function $\mathtt{p}$ permits us to define a preorder relation on the set $\mathfrak{D}$ of all qumixes.

3 The Toffoli and the Hadamard Gates

We will now investigate the basic algebraic properties of the Toffoli and of the Hadamard gates (the two elements of the Shi-Aharonov approximately universal set of gates).

The Toffoli gate represents the classical part of the Shi-Aharonov system: a classically universal gate, that permits us to define the reversible versions of all Boolean functions.

Definition 3.1 (The Toffoli gate) For any $n, m, p \geq 1$, the *Toffoli gate* is the linear operator $\mathtt{T}^{(n,m,p)}$ defined on $\bigotimes^{n+m+p} \mathbb{C}^2$ such that, for every element $|x_1, \ldots, x_n\rangle \otimes |y_1, \ldots, y_m\rangle \otimes |z_1, \ldots, z_p\rangle$ of the computational basis $\mathcal{B}^{(n+m+p)}$,

$$\begin{aligned}&\mathtt{T}^{(n,m,p)}(|x_1, \ldots, x_n\rangle \otimes |y_1, \ldots, y_m\rangle \otimes |z_1, \ldots, z_p\rangle)\\ &\quad = |x_1, \ldots, x_n\rangle \otimes |y_1, \ldots, y_m\rangle \otimes |z_1, \ldots, z_{p-1}, x_n y_m \widehat{+} z_p\rangle,\end{aligned}$$

where $\widehat{+}$ represents the sum modulo 2.

One can easily show that $\mathtt{T}^{(n,m,p)}$ is a unitary operator.

The Boolean functions $\mathtt{AND}$, $\mathtt{NAND}$, $\mathtt{NOT}$ can be now defined in terms of the Toffoli gate.

Definition 3.2

- For any $|\psi\rangle \in \bigotimes^n \mathbb{C}^2$ and for any $|\varphi\rangle \in \bigotimes^m \mathbb{C}^2$,

$$\mathtt{AND}(|\psi\rangle, |\varphi\rangle) := \mathtt{T}^{(n,m,1)}(|\psi\rangle \otimes |\varphi\rangle \otimes |0\rangle);$$

- For any $|\psi\rangle \in \bigotimes^n \mathbb{C}^2$ and for any $|\varphi\rangle \in \bigotimes^m \mathbb{C}^2$,

$$\mathtt{NAND}(|\psi\rangle, |\varphi\rangle) := \mathtt{T}^{(n,m,1)}(|\psi\rangle \otimes |\varphi\rangle \otimes |1\rangle);$$

- For any $|\psi\rangle \in \bigotimes^n \mathbb{C}^2$,

$$\mathtt{NOT}(|\psi\rangle) := \mathtt{NAND}(|\psi\rangle, |\psi\rangle).$$

Defining the Boolean negation NOT in terms of the Toffoli gate has, however, a shortcoming that is determined by the increasing of the dimension of the Hilbert space. Namely, if $|\psi\rangle$ belongs to $\bigotimes^n \mathbb{C}^2$, then its negation $\mathtt{NOT}(|\psi\rangle)$ belongs to $\bigotimes^{2n+1} \mathbb{C}^2$.

For computational aims, the following independent definition of the negation-gate is more economical:

Definition 3.3 (The negation) For any $n \geq 1$, the *negation* on $\bigotimes^n \mathbb{C}^2$ is the linear operator $\mathtt{Not}^{(n)}$ such that, for every element $|x_1, \ldots, x_n\rangle$ of the computational basis $\mathcal{B}^{(n)}$,

$$\mathtt{Not}^{(n)}(|x_1, \ldots, x_n\rangle) = |x_1, \ldots, x_{n-1}\rangle \otimes |1 - x_n\rangle.$$

We have:

$$\mathtt{Not}^{(n)} = \begin{cases} X, & \text{if } n = 1; \\ I^{(n-1)} \otimes X, & \text{otherwise,} \end{cases}$$

where X is the "first" Pauli matrix, i.e.,

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

The following lemma can be easily proved.

Lemma 3.1

(1) $\mathtt{T}^{(n,m,p)}\mathtt{Not}^{(n+m+p)} = \mathtt{Not}^{(n+m+p)}\mathtt{T}^{(n,m,p)}$;
(2) $\mathtt{T}^{(n,m,p)} = (I^{(n+m)} - P_1^{(n)} \otimes P_1^{(m)}) \otimes I^{(p)} + P_1^{(n)} \otimes P_1^{(m)} \otimes \mathtt{Not}^{(p)}$.

The Toffoli gate represents a classical reversible gate: whenever the input is a classical register, then also the output will be a classical register. In other words, the gate is incapable to "create" superpositions. The "genuine" quantum component of the Shi-Aharonov system is represented by the Hadamard gate (also called the *squareroot of the identity*).

Definition 3.4 (The squareroot of the identity) For any $n \geq 1$, the *squareroot of the identity* on $\bigotimes^n \mathbb{C}^2$ is the linear operator $\sqrt{\mathtt{I}}^{(n)}$ such that for every element $|x_1, \ldots, x_n\rangle$ of the computational basis $\mathcal{B}^{(n)}$:

$$\sqrt{\mathtt{I}}^{(n)}(|x_1, \ldots, x_n\rangle) = |x_1, \ldots, x_{n-1}\rangle \otimes \frac{1}{\sqrt{2}}((-1)^{x_n}|x_n\rangle + |1 - x_n\rangle).$$

The basic property of $\sqrt{\mathtt{I}}^{(n)}$ is the following:

$$\text{for any } |\psi\rangle \in \bigotimes^n \mathbb{C}^2, \quad \sqrt{\mathtt{I}}^{(n)}\left(\sqrt{\mathtt{I}}^{(n)}(|\psi\rangle)\right) = |\psi\rangle.$$

Clearly:

$$\sqrt{\mathtt{I}}^{(n)} = \begin{cases} H, & \text{if } n = 1; \\ I^{(n-1)} \otimes H, & \text{otherwise,} \end{cases}$$

where H is the Hadamard matrix:

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

By definition, gates are unitary operators whose domains consist of vectors of convenient Hilbert spaces. At the same time, gates can be naturally generalized also to qumixes. Such generalizations that transform qumixes into qumixes in a reversible way, are called *qumix-gates* (or *unitary quantum operations* [2]). Suppose that $\mathtt{G}$ is a gate of $\bigotimes^n \mathbb{C}^2$. Then the corresponding qumix-gate ${}^{\mathcal{D}}\mathtt{G}$ is defined as follows:

$${}^{\mathcal{D}}\mathtt{G}(\rho) := \mathtt{G}\rho\mathtt{G}^*,$$

where ρ is a density operator of $\bigotimes^n \mathbb{C}^2$ and $\mathtt{G}^*$ is the adjoint of $\mathtt{G}$. Accordingly, ${}^{\mathcal{D}}\mathtt{T}^{(m,n,p)}$ and ${}^{\mathcal{D}}\sqrt{\mathtt{I}}^{(n)}$ will represent the Toffoli and the Hadamard qumix-gates, respectively.

The following theorems describe some basic properties of our qumix-gates.

Theorem 3.1 [7]

(1) $\mathtt{p}({}^{\mathcal{D}}\mathtt{Not}^{(n)}(\rho)) = 1 - \mathtt{p}(\rho)$;
(2) $\mathtt{p}({}^{\mathcal{D}}\mathtt{AND}(\rho, \sigma)) = \mathtt{p}(\rho)\mathtt{p}(\sigma)$;
(3) $\mathtt{p}({}^{\mathcal{D}}\mathtt{NAND}(\rho, \sigma)) = 1 - \mathtt{p}(\rho)\mathtt{p}(\sigma)$.

Theorem 3.2 [5]

(1) *For any* $\rho \in \mathfrak{D}(\bigotimes^n \mathbb{C}^2)$: ${}^{\mathcal{D}}\sqrt{\mathtt{I}}^{(n)}({}^{\mathcal{D}}\sqrt{\mathtt{I}}^{(n)}(\rho)) = \rho$;
(2) $\forall n \in \mathbb{N}^+ : \mathtt{p}({}^{\mathcal{D}}\sqrt{\mathtt{I}}(k_n P_1^{(n)})) = \mathtt{p}({}^{\mathcal{D}}\sqrt{\mathtt{I}}(k_n P_0^{(n)})) = \frac{1}{2}$, *where* $k_n := \frac{1}{2^{n-1}}$.

Theorem 3.3 *Let* $\rho \in \mathfrak{D}(\bigotimes^n \mathbb{C}^2)$, $\sigma \in \mathfrak{D}(\bigotimes^m \mathbb{C}^2)$ *and* $\tau \in \mathfrak{D}(\bigotimes^p \mathbb{C}^2)$. *Then*,

$$\mathtt{p}\left({}^{\mathcal{D}}\mathtt{T}^{(n,m,p)}(\rho \otimes \sigma \otimes \tau)\right) = (1 - \mathtt{p}(\tau))\mathtt{p}(\rho)\mathtt{p}(\sigma) + \mathtt{p}(\tau)(1 - \mathtt{p}(\rho)\mathtt{p}(\sigma)).$$

Proof We have:

$$
\begin{aligned}
&\mathtt{p}\Big({}^{\mathcal{D}_{\mathtt{T}^{(n,m,p)}}}(\rho\otimes\sigma\otimes\tau)\Big)\\
&\quad=\mathtt{tr}\Big(P_1^{(n+m+p)}\mathtt{T}^{(n,m,p)}(\rho\otimes\sigma\otimes\tau)\mathtt{T}^{(n,m,p)}\Big)\\
&\quad=\mathtt{tr}\Big(P_1^{(n+m+p)}((I^{(n+m)}-I^{(n)}\otimes P_1^{(m)})\otimes I^{(p)}\\
&\qquad+P_1^{(n)}\otimes P_1^{(m)}\otimes\mathtt{Not}^{(p)})(\rho\otimes\sigma\otimes\tau)\\
&\qquad\times\Big(\Big(I^{(n+m)}-P_1^{(n)}\otimes P_1^{(m)}\Big)\otimes I^{(p)}\\
&\qquad+P_1^{(n)}\otimes P_1^{(m)}\otimes\mathtt{Not}^{(p)}\Big)\Big)\quad\text{(Theorem 3.1)}\\
&\quad=\mathtt{tr}\Big(\Big(\Big(I^{(n+m)}-I^{(n)}\otimes P_1^{(m)}\Big)\otimes P_1^{(p)}\\
&\qquad+P_1^{(n)}\otimes P_1^{(m)}\otimes P_1^{(p)}\mathtt{Not}^{(p)}\Big)(\rho\otimes\sigma\otimes\tau)\\
&\qquad\times\Big(\Big(I^{(n+m)}-P_1^{(n)}\otimes P_1^{(m)}\Big)\otimes I^{(p)}\\
&\qquad+P_1^{(n)}\otimes P_1^{(m)}\otimes\mathtt{Not}^{(p)}\Big)\Big)\quad\text{(by (2.1))}\\
&\quad=\mathtt{tr}\Big(\Big(\Big(I^{(n+m)}-P_1^{(n)}\otimes P_1^{(m)}\Big)\otimes I^{(p)}+P_1^{(n)}\otimes P_1^{(m)}\otimes\mathtt{Not}^{(p)}\Big)\\
&\qquad\times\Big(\Big(I^{(n+m)}-I^{(n)}\otimes P_1^{(m)}\Big)\otimes P_1^{(p)}\\
&\qquad+P_1^{(n)}\otimes P_1^{(m)}\otimes P_1^{(p)}\mathtt{Not}^{(p)}\Big)(\rho\otimes\sigma\otimes\tau)\Big)\\
&\quad=\mathtt{tr}\Big(\Big(\Big(I^{(n+m)}-P_1^{(n)}\otimes P_1^{(m)}\Big)\otimes P_1^{(p)}\\
&\qquad+P_1^{(n)}\otimes P_1^{(m)}\otimes\mathtt{Not}^{(p)}P_1^{(p)}\mathtt{Not}^{(p)}\Big)(\rho\otimes\sigma\otimes\tau)\Big)\\
&\quad=\mathtt{tr}\left(\left(I^{(n+m)}-P_1^{(n)}\otimes P_1^{(m)}\right)(\rho\otimes\sigma)\otimes P_1^{(p)}\tau\right)\\
&\qquad+\mathtt{tr}\left(P_1^{(m)}\rho\otimes P_1^{(m)}\sigma\otimes P_0^{(p)}\tau\right)\\
&\quad=\mathtt{tr}\left(\left(I^{(n+m)}-P_1^{(n)}\otimes P_1^{(m)}\right)(\rho\otimes\sigma)\right)\mathtt{tr}\left(P_1^{(p)}\tau\right)\\
&\qquad+\mathtt{tr}\left(P_1^{(m)}\rho\right)\mathtt{tr}\left(P_1^{(m)}\sigma\right)\mathtt{tr}\left(P_0^{(p)}\tau\right)\\
&\quad=\mathtt{tr}\left(\left(I^{(n+m)}-P_1^{(n)}\otimes P_1^{(m)}\right)(\rho\otimes\sigma)\right)\mathtt{tr}\left(P_1^{(p)}\tau\right)\\
&\qquad+\mathtt{tr}\left(P_1^{(m)}\rho\right)\mathtt{tr}\left(P_1^{(m)}\sigma\right)\mathtt{tr}\left(P_0^{(p)}\tau\right)\\
&\quad=(1-\mathtt{p}(\rho)\mathtt{p}(\sigma))\mathtt{p}(\tau)+\mathtt{p}(\rho)\mathtt{p}(\sigma)(1-\mathtt{p}(\tau)).
\end{aligned}
$$

□

As a consequence of Theorem 3.3 and of Theorem 3.1, the probability-value $\mathtt{p}({}^{\mathcal{D}}\mathtt{T}^{(n,m,p)}(\rho\otimes\sigma\otimes\tau))$ can be regarded as a kind of weighted sum of $\mathtt{p}({}^{\mathcal{D}}\mathtt{AND}(\rho,\sigma))$ and of $\mathtt{p}({}^{\mathcal{D}}\mathtt{NAND}(\rho,\sigma))$, with weight $\mathtt{p}({}^{\mathcal{D}}\mathtt{Not}^{(p)}(\tau))$ and $\mathtt{p}(\tau)$, respectively.

Theorem 3.4 *Let* $\rho\in\mathfrak{D}(\bigotimes^n\mathbb{C}^2)$. *Then*,

(1) $\sqrt{\mathtt{I}}^{(n)}P_1^{(n)}\sqrt{\mathtt{I}}^{(n)}=\frac{1}{2}I^{(n)}-\frac{1}{2}\mathtt{Not}^{(n)}$;

(2) $\mathtt{p}({}^{\mathcal{D}}\sqrt{\mathtt{I}}^{(n)}(\rho))=\frac{1}{2}-\frac{1}{2}\mathtt{tr}(\mathtt{Not}^{(n)}\rho)$.

Proof (1) One can easily show that $\sqrt{\mathtt{I}}^{(1)}P_1^{(1)}\sqrt{\mathtt{I}}^{(1)}=HP_1^{(1)}H=\frac{1}{2}I^{(1)}-\frac{1}{2}X=\frac{1}{2}I^{(1)}-\frac{1}{2}\mathtt{Not}^{(1)}$. Thus, by (2.1), we can conclude that $\sqrt{\mathtt{I}}^{(n)}P_1^{(n)}\sqrt{\mathtt{I}}^{(n)}=\frac{1}{2}I^{(n)}-\frac{1}{2}\mathtt{Not}^{(n)}$.

(2) The proof follows from (1). □

Theorem 3.5 *Let* $\rho\in\mathfrak{D}(\bigotimes^n\mathbb{C})$, $\sigma\in\mathfrak{D}(\bigotimes^m\mathbb{C})$ *and* $\tau\in\mathfrak{D}(\bigotimes^p\mathbb{C}^2)$. *Then*,

$$\mathtt{p}\Big({}^{\mathcal{D}}\sqrt{\mathtt{I}}^{(n+m+p)}\Big({}^{\mathcal{D}}\mathtt{T}^{(n,m,p)}(\rho\otimes\sigma\otimes\tau)\Big)\Big)=\mathtt{p}\Big({}^{\mathcal{D}}\sqrt{\mathtt{I}}^{(p)}(\tau)\Big).$$

Proof

$$\begin{aligned}
&\mathtt{p}\Big({}^{\mathcal{D}}\sqrt{\mathtt{I}}^{(n+m+p)}\Big({}^{\mathcal{D}}\mathtt{T}^{(n,m,p)}(\rho\otimes\sigma\otimes\tau)\Big)\Big)\\
&\quad=\mathtt{tr}\Big(\sqrt{\mathtt{I}}^{(n+m+p)}P_1^{(n+m+p)}\sqrt{\mathtt{I}}^{(n+m+p)}\mathcal{D}_{\mathtt{T}}(\rho\otimes\sigma\otimes\tau)\Big)\\
&\quad=\frac{1}{2}-\frac{1}{2}\mathtt{tr}\Big(\mathtt{Not}^{(n+m+p)}\mathtt{T}^{(n,m,p)}(\rho\otimes\sigma\otimes\tau)\mathtt{T}^{(n,m,p)}\Big)\quad\text{(Theorem 3.4(1))}\\
&\quad=\frac{1}{2}-\frac{1}{2}\mathtt{tr}\Big(\mathtt{Not}^{(n+m+p)}\Big(I^{(n+m+p)}-P_1^{(n)}\otimes P_1^{(m)}\otimes I^{(p)}\\
&\qquad+P_1^{(n)}\otimes P_1^{(m)}\otimes\mathtt{Not}^{(p)}\Big)(\rho\otimes\sigma\otimes\tau)\Big(I^{(n+m+p)}-P_1^{(n)}\otimes P_1^{(m)}\otimes I^{(p)}\\
&\qquad+P_1^{(n)}\otimes P_1^{(m)}\otimes\mathtt{Not}^{(p)}\Big)\Big)\quad\text{(Lemma 3.1(2))}\\
&\quad=\frac{1}{2}-\frac{1}{2}\mathtt{tr}\Big(\Big(\mathtt{Not}^{(n+m+p)}-P_1^{(n)}\otimes P_1^{(m)}\otimes\mathtt{Not}^{(p)}\\
&\qquad+P_1^{(n)}\otimes P_1^{(m)}\otimes\mathtt{Not}^{(p)}\mathtt{Not}^{(p)}\Big)\\
&\qquad(\rho\otimes\sigma\otimes\tau)\Big(I^{(n+m+p)}-P_1^{(n)}\otimes P_1^{(m)}\otimes I^{(p)}+P_1^{(n)}\otimes P_1^{(m)}\otimes\mathtt{Not}^{(p)}\Big)\Big)\\
&\quad=\frac{1}{2}-\frac{1}{2}\mathtt{tr}\Big(\Big(I^{(n+m+p)}-P_1^{(n)}\otimes P_1^{(m)}\otimes I^{(p)}+P_1^{(n)}\otimes P_1^{(m)}\otimes\mathtt{Not}^{(p)}\Big)
\end{aligned}$$

$$\Big(\mathtt{Not}^{(n+m+p)} - P_1^{(n)} \otimes P_1^{(m)} \otimes \mathtt{Not}^{(p)}$$

$$+ P_1^{(n)} \otimes P_1^{(m)} \otimes I^{(p)}\Big)(\rho \otimes \sigma \otimes \tau) \quad (\text{since } \mathtt{Not}^{(p)}\mathtt{Not}^{(p)} = I^{(p)})$$

$$= \frac{1}{2} - \frac{1}{2}\mathtt{tr}\left(\mathtt{Not}^{(n+m+p)}(\rho \otimes \sigma \otimes \tau)\right) = \mathtt{p}\left({}^{\mathcal{D}}\sqrt{\mathtt{I}}^{(p)}(\tau)\right) \quad \text{(Theorem 3.4(2).)}$$

□

4 Reversible and Irreversible Quantum Computational Structures

We will now introduce an algebraic structure whose domain is the set of all possible qumixes and whose operations are defined in terms of the Toffoli and of the Hadamard gates.

Definition 4.1 (The Shi-Aharonov quantum computational algebra) The *Shi-Aharonov quantum computational algebra* is the following structure

$$\left(\mathfrak{D}, \mathbb{T}, \sqrt{\mathbb{I}}, P_0^{(1)}, P_1^{(1)}, \frac{1}{2}I^{(1)}\right),$$

where:

- $\mathfrak{D}$ is the set of all qumixes;
- $\mathbb{T}$ is a ternary operation defined for any $\rho \in \mathfrak{D}(\bigotimes^n \mathbb{C}^2)$, for any $\sigma \in \mathfrak{D}(\bigotimes^m \mathbb{C}^2)$ and for any $\tau \in \mathfrak{D}(\bigotimes^p \mathbb{C}^2)$ as follows:

$$\mathbb{T}(\rho, \sigma, \tau) := {}^{\mathcal{D}}\mathtt{T}^{(n,m,p)}(\rho \otimes \sigma \otimes \tau);$$

- $\sqrt{\mathbb{I}}$ is a unary operation defined for any $\rho \in \mathfrak{D}(\bigotimes^n \mathbb{C}^2)$ as follows:

$$\sqrt{\mathbb{I}}(\rho) := {}^{\mathcal{D}}\sqrt{\mathtt{I}}^{(n)}(\rho);$$

- $P_0^{(1)}$, $P_1^{(1)}$, $\frac{1}{2}I^{(1)}$ are three special elements of $\mathfrak{D}(\mathbb{C}^2)$ that represent the privileged true, false and indeterminate qumix, respectively.

The set $\mathfrak{D}$ of all qumixes can be preordered by the relation $\preceq$ that is defined as follows.

Definition 4.2 (The qumix-preorder) For any $\rho \in \mathfrak{D}(\bigotimes^n \mathbb{C}^2)$ and any $\sigma \in \mathfrak{D}(\bigotimes^m \mathbb{C}^2)$,

$$\rho \preceq \sigma \quad \text{iff} \quad \mathtt{p}(\rho) \leq \mathtt{p}(\sigma) \quad \text{and} \quad \mathtt{p}\left({}^{\mathcal{D}}\sqrt{\mathtt{I}}^{(n)}(\rho)\right) \leq \mathtt{p}\left({}^{\mathcal{D}}\sqrt{\mathtt{I}}^{(m)}(\sigma)\right).$$

One can easily show that $\preceq$ is reflexive and transitive. This permits us to define, in the expected way, an equivalence relation $\equiv$ on the set $\mathfrak{D}$.

Definition 4.3 $\rho \equiv \sigma$ iff $\rho \preceq \sigma$ and $\sigma \preceq \rho$.

Consider now the set

$$[\mathfrak{D}]_{\equiv} := \{[\rho]_{\equiv} : \rho \in \mathfrak{D}\}.$$

Unlike qumixes (which are only preordered by $\preceq$), the equivalence-classes of $[\mathfrak{D}]_{\equiv}$ can be partially ordered in a natural way.

Definition 4.4

$$[\rho]_{\equiv} \preceq [\sigma]_{\equiv} \quad \text{iff} \quad \rho \preceq \sigma.$$

The relation $\preceq$ (which is well defined) is a partial order.

We will now consider a quotient-structure based on the quotient set $[\mathfrak{D}]_{\equiv}$.

Theorem 4.1 *$\equiv$ is a congruence relation with respect to $\mathbb{T}$ and $\sqrt{\mathbb{I}}$.*

Proof That $\sqrt{\mathbb{I}}$ is preserved by $\equiv$ is a consequence of the definition of $\equiv$. Suppose that $\rho_1 \equiv \rho_2$, $\sigma_1 \equiv \sigma_2$ and $\tau_1 \equiv \tau_2$. We have to show that $\mathbb{T}(\rho_1, \sigma_1, \tau_1) \equiv \mathbb{T}(\rho_2, \sigma_2, \tau_2)$. That $\mathfrak{p}(\mathbb{T}(\rho_1, \sigma_1, \tau_1)) = \mathfrak{p}(\mathbb{T}(\rho_2, \sigma_2, \tau_2))$ follows from the hypothesis and from Theorem 3.3. That $p(\sqrt{\mathbb{I}}(\mathbb{T}(\rho_1, \sigma_1, \tau_1))) = p(\sqrt{\mathbb{I}}(\mathbb{T}(\rho_2, \sigma_2, \tau_2)))$ follows from the hypothesis and from Theorem 3.5. □

On this basis we can define, in the expected way, the operations $\mathbb{T}$ and $\sqrt{\mathbb{I}}$ on $[\mathfrak{D}]_{\equiv}$. We obtain the following quotient-structure:

$$\left([\mathfrak{D}]_{\equiv}, \mathbb{T}, \sqrt{\mathbb{I}}, \left[P_0^{(1)}\right]_{\equiv}, \left[P_1^{(1)}\right]_{\equiv}, \left[\frac{1}{2}I^{(1)}\right]_{\equiv}\right).$$

5 The Complex Quantum Computational Algebra

We will now prove that the quotient of the Shi-Aharonov quantum computational algebra is isomorphic to a structure based on a particular set of complex numbers (the closed disc with center $(\frac{1}{2}, \frac{1}{2})$ and radius $\frac{1}{2}$). Let

$$\mathbb{C}_1 := \left\{(a, b) : a, b \in \mathbb{R} \text{ and } (1-2a)^2 + (1-2b)^2 \leq 1\right\}.$$

Note that for all pairs $(a, b) \in \mathbb{C}_1$, both elements a and b belong to the real interval $[0, 1]$.

Before introducing an algebraic structure on the set $\mathbb{C}_1$, let us first recall some properties of the set $\mathfrak{D}(\mathbb{C}^2)$ of all density operators of $\mathbb{C}^2$. As is well known, $\mathfrak{D}(\mathbb{C}^2)$ is in one-to-one correspondence with the set of all points of the Poincaré sphere. Consider a qumix τ of $\mathfrak{D}(\mathbb{C}^2)$ and let (t_1, t_2, t_3) be the point of the Poincaré sphere uniquely associated to τ. We have:

$$\tau = \frac{1}{2}\begin{pmatrix} 1+t_3 & t_1 - it_2 \\ t_1 + it_2 & 1-t_3 \end{pmatrix}.$$

One can easily see that:

$$\mathtt{p}(\tau) = \frac{1 - t_3}{2}$$

and

$$\mathtt{p}\Big({}^{\mathcal{D}}\sqrt{\mathtt{I}}(\tau)\Big) = \frac{1 - t_1}{2}.$$

Let $(a, b) \in \mathbb{C}_1$ and let $\rho(a, b)$ be the density operator associated to the triplet $(1 - 2b, 0, 1 - 2a)$. Thus,

$$\rho(a, b) = \begin{pmatrix} 1 - a & \frac{1}{2} - b \\ \frac{1}{2} - b & a \end{pmatrix}.$$

Clearly, $\mathtt{p}(\rho(a, b)) = a$ and $\mathtt{p}(\sqrt{\mathbb{I}}(\rho(a, b))) = b$.

On this basis, recalling Theorem 3.3, the following operations ($\mathbb{T}^{\mathbb{C}_1}$ and $\sqrt{\mathbb{I}}^{\mathbb{C}_1}$) can be naturally defined on the set $\mathbb{C}_1$:

Definition 5.1 (The pair Toffoli and the pair squareroot of the identity)

(1) $\mathbb{T}^{\mathbb{C}_1}((a_1, a_2), (b_1, b_2)(c_1, c_2)) = ((1 - c_1)a_1b_1 + c_1(1 - a_1b_1), c_2)$;
(2) $\sqrt{\mathbb{I}}^{\mathbb{C}_1}(a_1, a_2) = (a_2, a_1)$.

Lemma 5.1 *$\mathbb{C}_1$ is closed under $\mathbb{T}^{\mathbb{C}_1}$ and $\sqrt{\mathbb{I}}^{\mathbb{C}_1}$.*

Proof Easy computation. □

Consider now the structure

$$\mathcal{C}_1 = \Big(\mathbb{C}_1, \mathbb{T}^{\mathbb{C}_1}, \sqrt{\mathbb{I}}^{\mathbb{C}_1}, \underline{0}, \underline{1}, \underline{1/2}\Big),$$

where $\underline{0} := (0, \frac{1}{2})$, $\underline{1} := (1, \frac{1}{2})$ and $\underline{1/2} := (\frac{1}{2}, \frac{1}{2})$.

We will prove that $\mathcal{C}_1$ is isomorphic to

$$\left([\mathfrak{D}]_{\equiv}, \mathbb{T}, \sqrt{\mathbb{I}}, \left[P_0^{(1)}\right]_{\equiv}, \left[P_1^{(1)}\right]_{\equiv}, \left[\frac{1}{2}I^{(1)}\right]_{\equiv}\right).$$

Lemma 5.2

(1) $\rho(\mathbb{T}^{\mathbb{C}_1}((a_1, a_2), (b_1, b_2), (c_1, c_2))) = \mathbb{T}((\rho(a_1, a_2), \rho(b_1, b_2), \rho(c_1, c_2)))$;
(2) $\rho(\sqrt{\mathbb{I}}^{\mathbb{C}_1}((a_1, a_2))) = \sqrt{\mathbb{I}}(\rho(a_1, a_2))$.

Proof Easy computation. □

Theorem 5.1 *The structure $\mathcal{C}_1 = (\mathbb{C}_1, \mathbb{T}^{\mathbb{C}_1}, \sqrt{\mathbb{I}}^{\mathbb{C}_1}, \underline{0}, \underline{1}, \underline{1/2})$ is isomorphic to $([\mathfrak{D}]_{\equiv}, \mathbb{T}, \sqrt{\mathbb{I}}, [P_0^{(1)}]_{\equiv}, [P_1^{(1)}]_{\equiv}, [\frac{1}{2}I^{(1)}]_{\equiv})$.*

Proof (Along the lines of [3]).

Let h be the map of $\mathbb{C}_1$ into $[\mathfrak{D}]_{\equiv}$ such that for any $(a,b) \in \mathbb{C}_1$:

$$h((a,b)) := [\rho(a,b)]_{\equiv}.$$

The map is well defined (by definition of $\equiv$) and it is a homomorphism by Lemma 5.2.

We now prove that h is injective. Suppose that $h((a_1,a_2)) = h((b_1,b_2))$. Then $[\rho(a_1,a_2)]_{\equiv} = [\rho(b_1,b_2)]_{\equiv}$. Thus,

$$\mathtt{p}(\rho(a_1,a_2)) = \mathtt{p}(\rho(b_1,b_2)) \quad \text{and} \quad \mathtt{p}\left(\sqrt{\mathbb{I}}(\rho(a_1,a_2))\right) = \mathtt{p}\left(\sqrt{\mathbb{I}}(\rho(b_1,b_2))\right).$$

Therefore:

$$\mathtt{p}(\rho(a_1,a_2)) = a_1 = b_1 = \mathtt{p}(\rho(b_1,b_2))$$

and

$$\mathtt{p}\left(\sqrt{\mathbb{I}}(\rho(a_1,a_2))\right) = a_2 = b_2 = \mathtt{p}\left(\sqrt{\mathbb{I}}(\rho(b_1,b_2))\right).$$

Hence, $\rho(a_1,a_2) = \rho(b_1,b_2)$.

We now prove that h is surjective. Let ρ be a density operator in $\mathfrak{D}(\bigotimes^n \mathbb{C}^2)$ and let ρ_{red} be the reduced state of ρ to $\mathbb{C}^2$ (see [4]). We will show that

(1) $\mathtt{p}(\rho) = \mathtt{p}(\rho_{red})$;
(2) $\mathtt{p}(\sqrt{\mathbb{I}}(\rho)) = \mathtt{p}(\sqrt{\mathbb{I}}(\rho_{red}))$.

(1) By definition of reduced state, we have that for any self-adjoint operator A of $\mathbb{C}^2$, the following equality holds:

$$\mathtt{tr}\left(I^{(n-1)} \otimes A\rho\right) = \mathtt{tr}\left(A\rho_{red}\right). \tag{5.1}$$

Thus, $\mathtt{p}(\rho) = \mathtt{tr}(P_1^{(n)}\rho) = \mathtt{tr}(I^{(n-1)} \otimes P_1^{(1)}\rho) = \mathtt{tr}(P_1^{(1)}\rho_{red}) = \mathtt{p}(\rho_{red})$.

We now prove (2).

$$\begin{aligned}
\mathtt{p}\left(\sqrt{\mathbb{I}}(\rho)\right) &= \frac{1}{2} - \frac{1}{2}\mathtt{tr}\left(\mathtt{Not}^{(n)}\rho\right) \quad \text{(Theorem 3.4(2))} \\
&= \frac{1}{2} - \frac{1}{2}\mathtt{tr}\left(I^{(n-1)} \otimes \mathtt{Not}^{(1)}\rho\right) \\
&= \frac{1}{2} - \frac{1}{2}\mathtt{tr}\left(\mathtt{Not}^{(1)}\rho_{red}\right) \quad (5.1) \\
&= \mathtt{p}\left(\sqrt{\mathbb{I}}(\rho_{red})\right) \quad \text{(Theorem 3.4(2).)}
\end{aligned}$$

It follows that

$$[\rho]_{\equiv} = [\rho_{red}]_{\equiv}. \tag{5.2}$$

Let (a, b, c) be the point of the Poincaré sphere associated to ρ_{red}. Take $(\frac{1-c}{2}, \frac{1-a}{2}) \in \mathbb{C}_1$. Since $\mathfrak{p}(\rho(\frac{1-c}{2}\frac{1-a}{2})) = c$ and $\mathfrak{p}(\sqrt{\mathbb{I}}(\rho(\frac{1-c}{2}, \frac{1-a}{2}))) = a$, we obtain:

$$[\rho_{red}]_{\equiv} = h\left(\left(\frac{1-c}{2}, \frac{1-a}{2}\right)\right).$$

By (5.2), we can conclude that

$$[\rho]_{\equiv} = h\left(\left(\frac{1-c}{2}, \frac{1-a}{2}\right)\right).$$

Consequently h is surjective. □

On the basis of Theorem 5.1, one can say that the "logic" of the Shi-Aharonov system of quantum computational gates is nothing but a complex-valued logic.

References

1. Aharonov, D.: A simple proof that Toffoli and Hadamard are quantum universal, arXiv:quant-ph/0301040 (2003)
2. Aharonov, D., Kitaev, A., Nisan, N.: Quantum circuits with mixed states. In: STOC '98: Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing, pp. 20–30. ACM, New York (1998)
3. Cattaneo, G., Dalla Chiara, M.L., Giuntini, R., Leporini, R.: Quantum computational structures. Math. Slovaca **54**, 87–108 (2004)
4. Dalla Chiara, M.L., Giuntini, R., Leporini, R.: Quantum computational logics: A survey. In: Hendricks, V.F., Malinowski, J. (eds.) Trends in Logic: 50 Years of Studia Logica, pp. 213–255. Kluwer Academic, Dordrecht (2003)
5. Dalla Chiara, M.L., Giuntini, R., Leporini, R.: Logics from quantum computation. Int. J. Quant. Inf. **3**, 293–337 (2005)
6. Deutsch, D.: Quantum computational networks. Proc. R. Soc. Lond. A **425**, 73–90 (1989)
7. Gudder, G.: Quantum computational logics. Int. J. Theor. Phys. **42**, 39–47 (2003)
8. Nielsen, M., Chuang, I.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2000)
9. Shi, Y.: Both Toffoli and controlled—Not need little help to do universal quantum computation, arXiv:quant-ph/0205115 (2002)
10. Toffoli, T.: Reversible computing. In: de Bakker, J.W., van Leeuwen, J. (eds.) Automata, Languages and Programming, pp. 632–644. Springer, Berlin (1980)