J Philos Logic (2013) 42:467–481
DOI 10.1007/s10992-013-9271-9

The Toffoli-Hadamard Gate System: an Algebraic Approach

M. L. Dalla Chiara · A. Ledda · G. Sergioli · R. Giuntini

Received: 26 February 2010 / Accepted: 14 July 2012 / Published online: 6 April 2013

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. The basic algebraic properties of this system have been studied in Dalla Chiara et al. (Foundations of Physics 39(6):559–572, 2009), where we have introduced the notion of *Shi-Aharonov quantum computational structure*. In this paper we propose an algebraic abstraction from the Hilbert-space quantum computational structures, by introducing the notion of *Toffoli-Hadamard algebra*. From an intuitive point of view, such abstract algebras represent a natural quantum generalization of both classical and fuzzy-like structures.

Keywords Quantum logic · Universality · Quantum computational structures

1 Introduction

Classical computation theory satisfies a highly desirable property: it can be formulated in terms of a very small set of classical logical gates (Boolean functions),

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

A. Ledda (✉) · G. Sergioli · R. Giuntini
Dipartimento di Filosofia, Università di Cagliari, via Is Mirrionis 1,
09123 Cagliari, Italy
e-mail: antonio.ledda@unica.it

G. Sergioli
e-mail: giuseppe.sergioli@gmail.com

R. Giuntini
e-mail: giuntini@unica.it

called *(functionally) universal set of gates*. In the irreversible formulation of the gate-system it is sufficient to assume the single gate NAND, or the set consisting of the two gates AND and NOT, in order to gain all the Boolean functions. In the reversible version, such a role is played by a single gate: the *Toffoli gate* T (also called *controlled-controlled not*).

In quantum computation, gates are interpreted as unitary operators acting on pure states of a Hilbert space. Since unitary operators are uncountably many, there is no hope to find any finite *functionally universal* set of quantum gates. In other words, there is no finite set of quantum gates such that the behavior of any quantum gate G can be *exactly* reproduced by means of a convenient composition of gates belonging to the set. In spite of this, one can find finite sets S of quantum gates such that each S satisfies the following condition: the action of any quantum gate can be mathematically *approximated*, up to an arbitrary accuracy, via appropriate compositions of gates that belong to S [11]. Sets of gates that satisfy such a property are termed *approximately universal*.

Finding simpler and simpler approximate universal sets of 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: as a consequence of a theorem proved by Solovay and Kitaev [8], shifting from a universal set to another one only causes a polylogarithmic overhead. An important result obtained by Shi [15], and further investigated by Aharonov [1], has shown that the set whose elements are the (three-qubit) *Toffoli gate* and the (one-qubit) *Hadamard gate* (also called the *squareroot of the identity*) is approximately universal. Unlike the classical reversible case, the Toffoli gate is not sufficient to reproduce the behavior of all quantum gates. A gate exhibiting a "genuine"quantum character should be added: the squareroot of the identity comes into play.

All these results can be naturally extended to a more general approach (also called *quantum operational approach*), where pure states and unitary operators are replaced by mixed states (density operators) and by *unitary quantum operations*, respectively (see [12] and [2]). From a physical point of view, using mixed states (instead of pure states) has plenty of advantages. For instance, this allows us to treat more appropriately some critical problems that concern *measurements* in the middle of a computation, *decoherence* and *noise*.

The algebraic properties of the Shi-Aharonov universal set of gates (in the quantum operational version) have been investigated in [6], where the notion of *Shi-Aharonov quantum computational algebra* has been introduced. The quotient of this structure turns out to be isomorphic to a structure based on a particular set of complex numbers (the closed disc with center $(1/2, 1/2)$ and radius $1/2$). The price to pay is the loss of the reversible nature of the two quantum operations.

In this paper we propose an algebraic abstraction from the concrete quantum computational structures (investigated in [6]). To this aim, we introduce the notion of *Toffoli-Hadamard algebra*: an abstract structure equipped with two primitive operations (the *abstract Toffoli* and the *abstract Hadamard*) and three privileged elements, representing the *true*, the *false* and the *totally uncertain* piece of information, respectively. From an intuitive point of view, these abstract algebras can be regarded as a

kind of natural quantum generalization of both classical and fuzzy-like structures. In fact, we prove that any Toffoli-Hadamard algebra $\mathcal{A}$ has two special subdomains consisting of the *sharp elements* and of the *regular* elements, respectively. The *reduct* of $\mathcal{A}$, based on the set of all sharp elements, is a Boolean algebra, while the *reduct* of $\mathcal{A}$, based on the set of all regular elements, is a fuzzy-like structure.

2 Qubits, Quregisters and Qumixes

To keep the paper self-contained, we recall some basic notions of quantum computation. As is well known, the quantum homologous of the classical *bit* is the concept of *qubit*. 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 $\mathbb{C}^2$.

One may regard the basis elements $|0\rangle$ and $|1\rangle$ as the two classical truth-values *false* and *true* "wedged" by the complex numbers c_0 and c_1. Accordingly, a qubit is a *probabilistic superposition* of the two classical truth-values, where the *Falsity* has probability $|c_0|^2$, while the *Truth* has probability $|c_1|^2$. If the qubit represents the quantum counterpart of the classical bit (describing the pure state of a single particle), the quantum homologous of the classical *register* (corresponding to a system of n particles), is the *n-quregister*, a unit vector of the n-fold tensor product of the space $\mathbb{C}^2$:

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

$\left(\text{where } \bigotimes^1 \mathbb{C}^2 := \mathbb{C}^2\right)$. 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 $|x_1, \ldots, x_n\rangle$. The set $\mathcal{B}^{(n)} = \{|x_1, \ldots, x_n\rangle : x_i \in \{0, 1\}\}$ of all n-registers is an orthonormal basis for the space $\bigotimes^n \mathbb{C}^2$ (also called *computational basis* for the n-quregisters).

Quregisters are pure states, hence *maximal pieces of information*, that cannot be consistently extended to a richer knowledge. 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 $\mathfrak{D}\big(\bigotimes^n \mathbb{C}^2\big)$ the set of all qumixes of $\bigotimes^n \mathbb{C}^2$, while $\mathfrak{D} := \bigcup_{n=1}^{\infty}\big(\bigotimes^n \mathbb{C}^2\big)$ will denote the set of all possible qumixes. It can be seen that quregisters are special cases of qumixes.

As in the qubit-case, one can define a probability-function p assigning to any qumix ρ a probability-value. Intuitively, $\mathrm{p}(\rho)$ is the probability that the quantum information stored by ρ corresponds to a *true* information. To define the function 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 in any space $\bigotimes^n \mathbb{C}^2$ the *true* from the *false* registers:

$$|x_1, \ldots, x_n\rangle \text{ is called } \textit{true} \text{ iff } x_n = 1;$$
$$|x_1, \ldots, x_n\rangle \text{ is called } \textit{false} \text{ iff } x_n = 0.$$

In other words, the last bit of a given register determines its truth-value. Now, we can naturally define the *Falsity* and the *Truth* 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 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 the set of all true registers.

By applying the Born rule, the probability-function p can be defined as follows:

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

$$\mathrm{p}(\rho) := \mathrm{tr}\big(P_1^{(n)}\rho\big),$$

where tr is the trace-functional.

Clearly, $\mathrm{p}(\rho)$ represents the probability of the *truth-property* for state ρ. We will see how the function p induces a preorder-relation on the set $\mathfrak{D}$ of all qumixes.

3 The Toffoli and the Hadamard Gates

We will now define the two elements of the Shi-Aharanov gate-system: the Toffoli-gate (which is a classically universal gate), and the Hadamard-gate (which represents the genuine quantum component of the system).

Definition 3.1 (The Toffoli gate)
For any $n, m, p \geq 1$, the Toffoli gate is the linear operator $\mathrm{T}^{(n,m,p)}$ 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 $\mathcal{B}^{(n+m+p)}$,

$$\mathbf{T}^{(n,m,p)}\big(|x_1, \ldots, x_n\rangle \otimes |y_1, \ldots, y_m\rangle \otimes |z_1, \ldots, z_p\rangle\big) = |x_1, \ldots, x_n\rangle \otimes |y_1, \ldots, y_m\rangle \otimes |z_1, \ldots, z_{p-1}, x_n y_m \widehat{+} z_p\rangle,$$

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

Clearly, $\mathrm{T}^{(n,m,p)}$ is a unitary operator. On this basis, the Boolean functions AND, NAND, NOT can be defined via Toffoli.

Definition 3.2

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

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

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

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

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

$$\mathrm{NOT}\big(|\psi\rangle\big) := \mathrm{T}^{(1,1,n)}\big(|1\rangle, |1\rangle, |\psi\rangle\big).$$

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 $\mathrm{NOT}(|\psi\rangle)$ belongs to $\bigotimes^{n+2} \mathbb{C}^2$.

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 $\mathrm{Not}^{(n)}$ such that, for every element $|x_1, \ldots, x_n\rangle$ of the computational basis $\mathcal{B}^{(n)}$,

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

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.

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

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

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

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

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]).

Let G be a gate of $\bigotimes^n \mathbb{C}^2$. Then the corresponding qumix-gate ${}^{\mathcal{D}}\mathrm{G}$ is defined as follows:

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

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

Some basic properties of our gates are listed in the following theorems.

Theorem 3.1 [7, 10]

1. $\mathrm{p}\big({}^{\mathcal{D}}\mathrm{Not}^{(n)}(\rho)\big) = 1 - \mathrm{p}(\rho)$;
2. $\mathrm{p}\big({}^{\mathcal{D}}\mathrm{AND}(\rho, \sigma)\big) = \mathrm{p}(\rho)\mathrm{p}(\sigma)$;
3. $\mathrm{p}\big({}^{\mathcal{D}}\mathrm{NAND}(\rho, \sigma)\big) = 1 - \mathrm{p}(\rho)\mathrm{p}(\sigma)$,
4. *For any* $\rho \in \mathfrak{D}(\bigotimes^n \mathbb{C}^2)$: ${}^{\mathcal{D}}\sqrt{\mathrm{I}}^{(n)}\big({}^{\mathcal{D}}\sqrt{\mathrm{I}}^{(n)}(\rho)\big) = \rho$;
5. $\forall n \in \mathbb{N}^+ : \ \mathrm{p}\left({}^{\mathcal{D}}\sqrt{\mathrm{I}}\big(k_n P_1^{(n)}\big)\right) = \mathrm{p}\left({}^{\mathcal{D}}\sqrt{\mathrm{I}}\big(k_n P_0^{(n)}\big)\right) = \frac{1}{2}$, *where* $k_n := \frac{1}{2^{n-1}}$.

Theorem 3.2 [6] *Let* $\rho \in \mathfrak{D}\big(\bigotimes^n \mathbb{C}^2\big)$, $\sigma \in \mathfrak{D}\big(\bigotimes^m \mathbb{C}^2\big)$ *and* $\tau \in \mathfrak{D}\big(\bigotimes^p \mathbb{C}^2\big)$. *Then,*

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

As a consequence of Theorems 3.2 and 3.1, the probability-value $\mathrm{p}\big({}^{\mathcal{D}}\mathrm{T}^{(n,m,p)}(\rho \otimes \sigma \otimes \tau)\big)$ can be regarded as a kind of weighted sum of $\mathrm{p}\big({}^{\mathcal{D}}\mathrm{AND}(\rho, \sigma)\big)$ and of $\mathrm{p}\big({}^{\mathcal{D}}\mathrm{NAND}(\rho, \sigma)\big)$, with weight $\mathrm{p}\big({}^{\mathcal{D}}\mathrm{Not}^{(p)}(\tau)\big)$ and $\mathrm{p}(\tau)$, respectively.

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

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

4 Reversible and Irreversible Quantum Computational Structures

We will first recall the main features of the *Shi-Aharonov quantum computational algebra*: a concrete 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 (see [6]).

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

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

where:

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

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

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

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

- $P_0^{(1)}$, $P_1^{(1)}$, $\frac{1}{2}I^{(1)}$ (where $I^{(1)}$ is the identity operator of $\mathbb{C}^2$) 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 $\rho, \sigma \in \mathfrak{D}$,

$$\rho \preceq \sigma \text{ iff } \mathrm{p}(\rho) \leq \mathrm{p}(\sigma) \text{ and } \mathrm{p}\left(\sqrt{\mathbb{I}}(\rho)\right) \leq \mathrm{p}\left(\sqrt{\mathbb{I}}(\sigma)\right).$$

One can easily see 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:

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

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 $\sqrt{\mathbb{I}}$.*

Thanks to Theorem 4.1, we can define, in the expected way, the operations $\mathbb{T}$ and $\sqrt{\mathbb{I}}$ on $[\mathfrak{D}]_{\equiv}$. Hence, we obtain the following quotient-structure:

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

While $\mathcal{SA}$ is a reversible quantum computational structure, its quotient $\mathcal{SA}_{\equiv}$ is clearly irreversible.

Interestingly enough, the quotient-structure $\mathcal{SA}_{\equiv}$ turns out to be isomorphic to a structure based on a particular set of complex numbers: the closed disc with center $\left(\frac{1}{2}, \frac{1}{2}\right)$ and radius $\frac{1}{2}$ ([6]).

As is well known, $\mathfrak{D}(\mathbb{C}^2)$ is in one-to-one correspondence with the set of all points of the Bloch-Poincaré sphere (of radius 1).Consider a qumix τ of $\mathfrak{D}(\mathbb{C}^2)$ and let (t_1, t_2, t_3) be the point of the Bloch-Poincaré sphere that is uniquely associated to τ. We have (Fig. 1):

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

One can easily see that:

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

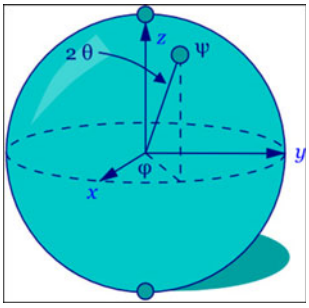

Fig. 1 The Bloch-Poincaré sphere

and

$$\mathrm{p}\left(\sqrt{\mathbb{I}}(\tau)\right) = \frac{1-t_1}{2}.$$

Apparently, the coordinate t_2 is uninfluential with respect to $\mathrm{p}(\tau)$ and $\mathrm{p}\left(\sqrt{\mathbb{I}}(\tau)\right)$. This suggests to shift down one dimension. Accordingly, we define the following set of complex numbers:

$$\mathbb{C}_1 := \left\{\left(\mathrm{p}(\tau)\right),\ \mathrm{p}\left(\sqrt{\mathbb{I}}(\tau)\right)\right) \ :\ \tau \in \mathfrak{D}\left(\mathbb{C}^2\right)\right\}.$$

One can easily show that:

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

On this basis, recalling Theorem 3.2, a Toffoli-like operation $\left(\mathbb{T}^{\mathbb{C}_1}\right)$ and a Hadamard-like operation $\left(\sqrt{\mathbb{I}}^{\mathbb{C}_1}\right)$ can be naturally defined on the set $\mathbb{C}_1$.

Definition 4.4 (The pair-Toffoli and the pair-Hadamard)

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. $\sqrt{\mathbb{I}}^{\mathbb{C}_1}(a_1,a_2) = (a_2,a_1)$.

Consider now the structure

$$\mathcal{C}_1 = \left(\mathbb{C}_1\,, \mathbb{T}^{\mathbb{C}_1}\,, \sqrt{\mathbb{I}}^{\mathbb{C}_1}\,, \underline{0}\,, \underline{1}\,, \underline{\frac{1}{2}}\right), \tag{1}$$

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

We will call $\mathcal{C}_1$ the *complex Shi-Aharonov quantum computational algebra*.

Theorem 4.2 [6] *The complex Shi-Aharonov quantum computational algebra is isomorphic to the quotient of the Shi-Aharonov quantum computational algebra.*

The primitive operations of the structure $\mathcal{C}_1$ permit us to define three important new operations: the *product*, the *negation* and the *probabilistic sum*.

Definition 4.5 (The product, the negation and the probabilistic sum)

1. $(a_1,a_2)\cdot(b_1,b_2) := \mathbb{T}^{\mathbb{C}_1}\left((a_1,a_2),(b_1,b_2),\underline{0}\right)$;
2. $(a_1,a_2)' := \mathbb{T}^{\mathbb{C}_1}(\underline{1},\underline{1},(a_1,a_2))$;
3. $(a_1,a_2)\boxplus(b_1,b_2) := \left((a_1,a_2)'\cdot(b_1,b_2)'\right)'$.

The following Lemma sums up some interesting properties of $\mathcal{C}_1$.

Lemma 4.1

1. $(a_1,a_2)\cdot(b_1,b_2) = \left(a_1b_1, \frac{1}{2}\right)$;
2. $(a_1,a_2)\boxplus(b_1,b_2) = \left(a_1+b_1-a_1b_2, \frac{1}{2}\right)$;
3. $(a_1,a_2)' = (1-a_1,a_2)$;

4. $\cdot$ *is associative and commutative;*
5. *Generally,* $(a_1, a_2) \cdot \underline{1} \neq (a_1, a_2)$*;*
6. $\sqrt{\mathbb{I}}^{\mathbb{C}_1}\left(\sqrt{\mathbb{I}}^{\mathbb{C}_1}((a_1, a_2))\right) = (a_1, a_2)$*;*
7. $\sqrt{\mathbb{I}}^{\mathbb{C}_1}\left(\underline{\frac{1}{2}}\right) = \underline{\frac{1}{2}}$*;*
8. $\sqrt{\mathbb{I}}^{\mathbb{C}_1}(\underline{0}) \cdot \underline{1} = \underline{\frac{1}{2}}$.

Proof Straightforward. □

5 The Toffoli-Hadamard Algebra

We will now "distill" an algebraic abstraction from the concrete structure $\mathcal{C}_1$ (investigated in the previous section). To this aim we will introduce the notion of *Toffoli-Hadamard algebra*: an abstract structure equipped with two primitive operations (the *abstract Toffoli* and the *abstract Hadamard*) and three privileged elements, representing the *true*, the *false* and the *totally uncertain* piece of information, respectively.

Definition 5.1 (Toffoli-Hadamard algebra)
A Toffoli-Hadamard algebra is a structure $\mathrm{A} = \left(A, t, \sqrt{I}, 0, 1, k\right)$ of type $\langle 3, 1, 0, 0, 0\rangle$ where the operations product $(\cdot)$, negation $(')$, probabilistic sum $(\boxplus)$ are defined as follows (for any $x, y \in A$):

- $x \cdot y := t(x, y, 0)$;
- $x' := t(1, 1, x)$;
- $x \boxplus y := \left(x' \cdot y'\right)'$.

The structure shall satisfy the following axioms:

T1	$t(x, y, z) = t(y, x, z)$	(left commutativity)
T2	$t(x, 1, t(y, 1, z)) = t(t(x, 1, y), 1, z)$	(1-associativity)
T3	$t(x, 0, y) = y$	
T4	$t(x \cdot y, z, w) = t(x, y \cdot z, w)$	(strong associativity)
T5	$t\big(x, y, t(z, w, r)\big) = t\big(z, w, t(x, y, r)\big)$	(double exchange)
T6	$x'' = x$	(double negation)
T7	$0' = 1$	
T8	$(x \cdot 1)' = (x' \cdot 1)$	(smoothness)
T9	$t(x, y, z) \cdot 1 = t(x, y, z \cdot 1)$	(1-import export)
T10	$x \boxplus \big(y \cdot (x' \cdot y')\big) = (x \boxplus y) \cdot (x \boxplus y')$	(conditional distributivity)
T11	$\big((x \boxplus (x \cdot y')\big) \cdot y = \big(y \boxplus (x' \cdot y)\big) \cdot x$	(conditional Łukasiewicz)
T12	$t(x, y, k) = k$	
T13	$\sqrt{I}\big(\sqrt{I}(x)\big) = x$	(double squareroot of the identity)
T14	$\sqrt{I}(k) = k$	(fixpoint)
T15	$\sqrt{I}(0) \cdot 1 = k$	
T16	$\sqrt{I}\big(t(x, y, z)\big) \cdot 1 = \sqrt{I}(z) \cdot 1$.	

One can easily show that the concrete structure $\mathcal{C}_1$(the *complex Shi-Aharonov quantum computational algebra*) satisfies the axioms of Toffoli-Hadamard algebras. Accordingly, we will also call $\mathcal{C}_1$ the *standard Toffoli-Hadamard algebra*.

The following Lemma sums up some important properties of Toffoli-Hadamard algebras.

Lemma 5.1 *Let* $\mathcal{A} = \left(A, t, \sqrt{I}, 0, 1, k\right)$ *be a Toffoli-Hadamard algebra.*

1. *the product* $\cdot$ *is commutative and associative;*
2. *generally,* $x \cdot 1 \neq x$*;*
3. $(x \cdot y) \cdot 1 = x \cdot y$*;*
4. *t satisfies the "Toffoli-truth table":*
   $t(0,0,0) = 0;\ t(0,0,1) = 1;\ t(0,1,0) = 0;\ t(0,1,1) = 1;$
   $t(1,0,0) = 0;\ t(1,0,1) = 1;\ t(1,1,0) = 1;\ t(1,1,1) = 0;$
5. $t(x \cdot 1, y \cdot 1, z \cdot 1) = t(x, y, z) \cdot 1$*;*
6. $\sqrt{I}\left(\sqrt{I}(x) \cdot 1\right) \cdot 1 = k$*;*
7. $\sqrt{I}(x \cdot 1) \cdot 1 = k$*;*
8. $x' \cdot 1 = \sqrt{I}\left(t\left(1, 1, \sqrt{I}(t\ (1, 1, x))\right)\right)$.

Proof

(1) The commutativity of $\cdot$ is a consequence of **T1**. As to associativity, we have (by **T4**): $x \cdot (y \cdot z) = t(x, t(y, z, 0), 0) = t(t(x, y, 0), z, 0) = (x \cdot y) \cdot z$.

(2) Follows from Lemma 4.1-(5).

(3) We have (by **T9**, **T1**, and **T3**): $(x \cdot y) \cdot 1 = t(t(x, y, 0), 1, 0) = t(x, y, t(0, 1, 0)) = t(x, y, t(1, 0, 0)) = t(x, y, 0) = x \cdot y$.

(4) By **T3** and **T1**.

(5) We have:

$$
\begin{aligned}
t(x \cdot 1, y \cdot 1, z \cdot 1) &= t(t(x, 1, 0), t(y, 1, 0), t(z, 1, 0)) \\
&= t(t(t(x, 1, 0), y, 0), 1, t(z, 1, 0)) && \textbf{(T4)} \\
&= t(t(y, t(x, 1, 0), 0), 1, t(z, 1, 0)) && \textbf{(T1)} \\
&= t(t(t(y, x, 0)1, 0), 1, t(z, 1, 0))) && \textbf{(T4)} \\
&= t(t(y, x, t(0, 1, 0)), 1, t(z, 1, 0)) && \textbf{(T9)} \\
&= t(t(y, x, 0), 1, t(z, 1, 0)) && \text{(item-(4))} \\
&= t(t(x, y, 0), 1, t(z, 1, 0)) && \textbf{(T1)} \\
&= t(z, 1, t(t(x, y, 0), 1, 0)) && \textbf{(T5)} \\
&= t(z, 1, x \cdot y \cdot 1) && \textbf{(T9)} \text{ and item-(4))} \\
&= t(z, 1, x \cdot y) && \text{(item-(3))} \\
&= t(z, 1, t(x, y, 0)) \\
&= t(x, y, t(z, 1, 0)) && \textbf{(T5)} \\
&= t(t(x, y, z), 1, 0)) && \textbf{(T9)} \\
&= t(x, y, z) \cdot 1.
\end{aligned}
$$

(6) We have (by **T16** and **T15**): $\sqrt{I}\left(\sqrt{I}(x)\cdot 1\right)\cdot 1 = \sqrt{I}\left(\left(t\left(\sqrt{I}(x),1,0\right)\right)\right)\cdot 1 = \sqrt{I}(0)\cdot 1 = k$.

(7) Along the lines of (6).

(8)

$$\begin{aligned}\sqrt{I}(t(1,1,\sqrt{I}(t(1,1,x))))\cdot 1 &= \sqrt{I}\left(\sqrt{I}(t(1,1,x))\right)\cdot 1 && (\mathbf{T16})\\ &= t(1,1,x)\cdot 1 && (\mathbf{T13})\\ &= x'\cdot 1 && (\text{by definition of } ')\end{aligned}$$

□

As we have seen, the certain piece of information 1 does not represent a neutral element for a Toffoli-Hadamard algebra. In this situation, it is interesting to isolate the subset of the algebra consisting of all elements for which 1 is a neutral element. Accordingly, given $\mathcal{A} = \left(A, t, \sqrt{I}, 0, 1, k\right)$, we define the following set

$$\mathcal{R}(\mathcal{A}) := \{x \in A : x\cdot 1 = x\},$$

which will be called the set of the *regular* elements of $\mathcal{A}$. One can easily show that $\mathcal{R}(\mathcal{A})$ is always non-empty.

In the standard Toffoli-Hadamard algebra $\mathcal{C}_1$ the regular elements have a canonical form. One can prove that:

$$\mathcal{R}(\mathcal{C}_1) = \{(a, 1/2) : a \in \mathbb{R},\ 0 \leq a \leq 1\}.$$

Thus, $\mathcal{R}(\mathcal{C}_1)$ turns out to be in one-to-one correspondence with the real interval $[0, 1]$, which represents the "fuzzy" part of the disc. One can easily see that $\mathcal{R}(\mathcal{C}_1)$ is closed under the Toffoli-operation $\mathbb{T}^{\mathbb{C}_1}$. At the same time, $\mathcal{R}(\mathcal{C}_1)$ is not closed under the Hadamard-operation $\sqrt{\mathbb{I}}^{\mathbb{C}_1}$, which represents a genuine "disc-operation".

Interestingly enough, for any Toffoli-Hadamard algebra $\mathcal{A}$, $\mathcal{R}(\mathcal{A})$ is closed under the negation operation.

Lemma 5.2 *If $x \in \mathcal{R}(\mathcal{A})$, then $x' \in \mathcal{R}(\mathcal{A})$.*

Proof By definition of the operation $'$, we have: $x'\cdot 1 = t(1,1,x)\cdot 1$. By **T9**, we obtain: $t(1,1,x)\cdot 1 = t(1,1,x\cdot 1)$. Since x is regular, we can conclude that: $x'\cdot 1 = t(1,1,x) = x'$. □

Besides the regular elements, two other important subdomains of a Toffoli Hadamard algebra $\mathcal{A}$ are represented by the set $\mathcal{I}(\mathcal{A})$ of all *idempotent* elements and by the set $\mathcal{S}(\mathcal{A})$ of all *sharp* elements, respectively. These two sets are defined as follows:

- $\mathcal{I}(\mathcal{A}) := \{x \in A : x\cdot x = x\}$;
- $\mathcal{S}(\mathcal{A}) := \{x \in \mathcal{R}(\mathcal{A}) : x\cdot x' = 0\}$.

Theorem 5.1 *In any Toffoli-Hadamard algebra $\mathcal{A}$:*

$$\mathcal{I}(\mathcal{A}) \subseteq \mathcal{R}(\mathcal{A}).$$

Proof If $x \in \mathcal{I}(\mathcal{A})$, then (by Lemma 5.1-(3)), $x = x \cdot x = x \cdot x \cdot 1 = x \cdot 1$, whence $x \in \mathcal{R}(\mathcal{A})$. □

In the particular case where $\mathcal{A}$ is the standard Toffoli-Hadamard algebra $\mathcal{C}_1$ we obtain:

$$\mathcal{I}(\mathcal{C}_1) = \mathcal{S}(\mathcal{C}_1) = \{0, 1\}.$$

In other words, both the set of the idempotent elements and the set of the sharp elements collapse into the certainty- set $\{0, 1\}$. At the same time,

$$\mathcal{I}(\mathcal{C}_1) \subset \mathcal{R}(\mathcal{C}_1).$$

Interestingly enough, there are examples of abstract $\mathcal{A}$'s such that

$$\mathcal{S}(\mathcal{A}) \subset \mathcal{I}(\mathcal{A}).$$

However notice that, in general, $\mathcal{S}(\mathcal{A}) \not\subseteq \mathcal{I}(\mathcal{A})$, as the following example shows:

Example 5.1 Let $\mathcal{Q} = \Big([0, 1]^2, t, \sqrt{I}, \underline{0}, \underline{1}\Big)$, where:

1. $t\big((a_1, a_2), (b_1, b_2)(c_1, c_2)\big) = \big((1 - c_1)a_1b_1 + c_1(1 - a_1b_1), c_2\big)$;
2. $\sqrt{I}(a_1, a_2) = (a_2, a_1)$;
3. $\underline{0} = \big(0, \frac{1}{2}\big)$ and $\underline{1} = \big(1, \frac{1}{2}\big)$;
4. $(a_1, a_2) \cdot (b_1, b_2) = t\big((a_1, a_2), (b_1, b_2), \underline{0}\big)$;
5. $(a_1, a_2)' = t\big(\underline{1}, \underline{1}, (a_1, a_2)\big)$.

One verifies that $\mathcal{Q}$ is a Toffoli-Hadamard algebra.
Consider $\big(0, \frac{1}{4}\big)$. One sees that $\big(0, \frac{1}{4}\big) \cdot \big(0, \frac{1}{4}\big)' = \big(0, \frac{1}{4}\big) \cdot \big(1, \frac{1}{4}\big) = \big(0, \frac{1}{2}\big) = \underline{0}$. But $\big(0, \frac{1}{4}\big)^2 = \big(0, \frac{1}{2}\big) = \underline{0} \neq \big(0, \frac{1}{4}\big)$, and $\big(0, \frac{1}{4}\big) \cdot \underline{1} = \underline{0} \neq \big(0, \frac{1}{4}\big)$.

In the abstract case one can prove that the sharp elements of any Toffoli-Hadamard algebra have a classical Boolean behavior.

Theorem 5.2 *Let $\mathcal{A}$ be a Toffoli-Hadamard algebra. The reduct*

$$(\mathcal{S}(\mathcal{A}) \cap \mathcal{I}(\mathcal{A}),\ \cdot\ ,\ \boxplus\ ,\ \neg,\ 1\ ,\ 0)$$

is a Boolean algebra.

Proof Let us first prove the following Lemma: □

Lemma 5.3 *Let $\mathcal{A}$ be a Toffoli-Hadamard algebra. For any $x, y \in \mathcal{S}(\mathcal{A})$, we have:*

1. $x = (x \boxplus y) \cdot (x \boxplus \neg y)$;
2. $(x \boxplus \neg y) \cdot y = (y \boxplus \neg x) \cdot x$;
3. $\mathcal{S}(\mathcal{A})$ *is closed under* $\neg, \cdot, \boxplus$.

Proof of Lemma 5.3

(1) $x = x \boxplus 0 = x \boxplus (y \cdot \neg y) = x \boxplus (y \cdot (\neg y \cdot \neg x)) = (x \boxplus y) \cdot (x \boxplus \neg y)$ (by **T10**).
(2) $x = (x \boxplus y) \cdot (x \boxplus \neg y)$ and $y = (x \boxplus y) \cdot (y \boxplus \neg x)$ (by item-(1)). Whence, $(y \boxplus \neg x) \cdot x = (x \boxplus y) \cdot (x \boxplus \neg y) \cdot (y \boxplus \neg x) = (x \boxplus \neg y) \cdot y$ (again by item-(1)).
(3) The closure under $\neg$ is straightforward. Let $x, y \in \mathcal{S}(\mathcal{A})$. Then, $(x \cdot y) \cdot \neg(x \cdot y) = x \cdot (y \cdot (\neg x \boxplus \neg y)) = x \cdot (\neg x \cdot (x \boxplus y)) = 0$ (by item-(2)). Whence, $\mathcal{S}(\mathcal{A})$ is closed under $\cdot$, and, consequently, under $\boxplus$ also.

Q.E.D. (Lemma 5.3)

Let us now prove the Theorem. Let $\mathcal{A}$ be a Toffoli-Hadamard algebra. Then, both structures $(\mathcal{S}(\mathcal{A}) \cap \mathcal{I}(\mathcal{A}), \boxplus, 0)$ and $(\mathcal{S}(\mathcal{A}) \cap \mathcal{I}(\mathcal{A}), \cdot, 1)$ are commutative monoids (in virtue of Lemma 5.1 and of Lemma 5.3-(3)). Furthermore, for any $x \in \mathcal{S}(\mathcal{A})$, $x \boxplus \neg x = 1$. By Lemma 5.3-(2), the Łukasiewicz-axiom holds. Since $\mathcal{I}(\mathcal{A}) \subseteq \mathcal{R}(\mathcal{A})$, we obtain that the reduct $(\mathcal{S}(\mathcal{A}) \cap \mathcal{I}(\mathcal{A}), \cdot, \neg, 1, 0)$ is an MV-algebra. We also have: $x \cdot x = x$. On this basis, we can conclude that the structure $(\mathcal{S}(\mathcal{A}) \cap \mathcal{I}(\mathcal{A}), \cdot, \boxplus, \neg, 1, 0)$ is a Boolean algebra [4]. □

6 Open Problems

We close the paper by focusing upon five open problems:

- Are the axioms of Toffoli-Hadamard algebras independent?
- Does the variety generated by the standard (disc) structure coincide with the variety of all Toffoli-Hadamard algebras?
- Investigate some quasi-varieties of Toffoli-Hadamard algebras, where some relevant properties of the standard algebra (*cancellation law*, *no zero division condition*,....) are satisfied.
- Develop an independent axiomatization of *Toffoli algebras* in the signature of t, only.
- Compare Toffoli-algebras with some other well known fuzzy structures (say, *product MV algebras*, where the product $\cdot$ is a primitive operation).

References

1. Aharonov, D. (2003). A simple proof that Toffoli and Hadamard are quantum universal. arXiv: quant-ph/0301040.
2. Aharonov, D., Kitaev, A., Nisan, N. (1998). Quantum circuits with mixed states. *In STOC '98: Proceedings of the thirtieth annual ACM symposium on Theory of computing* (pp. 20–30). ACM Press.
3. Cattaneo, G., Dalla Chiara, M.L., Giuntini, R., Leporini R. (2004). Quantum computational structures. *Mathematica Slovaca*, *54*, 87–108.
4. Cignoli, R., D'Ottaviano I.M.L., Mundici, D. (2000). *Algebraic foundations of many-valued reasoning*. Dordrecht: Kluwer.
5. Dalla Chiara, M.L., Giuntini, R., Leporini, R. (2003). Quantum computational logics: a survey In V.F. Hendricks & J. Malinowski (Eds.), *Trends in logic: 50 years of studia logica* (pp. 213–255). Dordrecht: Kluwer.

6. Dalla Chiara, M.L., Giuntini, R., Freytes, H., Ledda, A., Sergioli, G. (2009). The algebraic structure of an approximately universal system of quantum computational gates. *Foundations of Physics*, *39*(6), 559–572.
7. Dalla Chiara, M.L., Giuntini, R., Leporini, R. (2005). Logics from Quantum Computation. *International Journal of Quantum Information*, *3*, 293–337.
8. Dawson, C.M., & Nielsen, M.A. (2005). The Solovay-Kitaev algorithm. arXiv:quant-ph/0505030.
9. Deutsch, D. (1989). Quantum computational networks. *Proceedings of the Royal Society of London A*, *425*, 73–90.
10. Gudder, G. (2003). Quantum computational logics. *International Journal of Theoretical Physics, 42*, 39–47.
11. Kitaev, A.Y. (1997). Quantum computations: algorithms and error correction. *Russian Mathematical Surveys*, *52*(6), 1191–1249.
12. Kraus, K. (1983). *States effects and operations*. Berlin: Springer-Verlag.
13. Ledda, A., Konig, M., Paoli, F., Giuntini, R. (2006). MV algebras quantum computation. *Studia Logica*, *82*(2), 245–270.
14. Nielsen, M., & Chuang, I. (2000). *Quantum computation and quantum information*. Cambridge: Cambridge University Press.
15. Shi, Y. (2002). Both Toffoli and controlled-Not need little help to do universal quantum computation. arXiv:quant-ph/0205115.
16. Toffoli, T. (1980). Reversible computing. In J.W. de Bakker & J. van Leeuwen (Eds.), *Automata, Languages and Programming* (632–644). Berlin: Springer.