# FUZZY APPROACH FOR TOFFOLI GATE IN QUANTUM COMPUTATION WITH MIXED STATES

HECTOR FREYTES

Dipartimento di Matematica e Informatica “Ulisse Dini", Universitá di Firenze,
Viale Morgagni 67a, Firenze, Italia
Departamento de Matemática UNR-CONICET, Av. Pellegrini 250, CP 2000 Rosario, Argentina
Universitá di Cagliari, Via Is Mirrionis 1, 09123 Cagliari, Italy
(e-mails: hfreytes@gmail.com, hfreytes@dm.uba.ar)

and

GIUSEPPE SERGIOLI

Universitá di Cagliari, Via Is Mirrionis 1, 09123 Cagliari, Italy
(e-mail: giuseppe.sergioli@gmail.com)

(*Received April 11, 2014 – Revised August 26, 2014*)

In the framework of quantum computation with mixed states, a fuzzy representation based on continuous $t$-norms for Toffoli gate is introduced. In this representation, the incidence of nonseparability is specially investigated.

**PACS numbers:** 03.67.Lx, 02.10.-v

**Keywords:** Toffoli gate, density operators, continuous $t$-norms, fuzzy logic.

## Introduction

Standard quantum computing is based on quantum systems described by finite-dimensional Hilbert spaces, specially $\mathbb{C}^2$, that is the two-dimensional space where qubits live. A qubit (the quantum counterpart of the classical bit) is represented by a unit vector in $\mathbb{C}^2$ and, generalizing for a positive integer $n$, $n$-qubits are represented by unit vectors in $\otimes^n\mathbb{C}^2$. Similarly to the classical case, it is possible to study the behaviour of a number of quantum logical gates (hereafter quantum gates, for short) operating on qubits. These quantum gates are represented by unitary operators.

In [2, 3] a quantum gate system based on Toffoli gate is studied. This system is interesting for two main reasons: (i) it is related to continuous $t$-norms [15], i.e. continuous binary operations on the interval [0, 1] that are commutative, associative, nondecreasing and with 1 as the unit element. They are naturally proposed in fuzzy logic as interpretations of the conjunction [13]. (ii) A generalization of the mentioned system to mixed states allows us to connect it with sequential effect algebras [10], introduced to study the sequential action of quantum effects which are unsharp versions of quantum events [11, 12].

The aim of this paper is to study a probabilistic type representation of Toffoli gate based on Łukasiewicz negation $\neg x = 1 - x$, Łukasiewicz sum $x \oplus y = \min x + y, 1$ and product $t$-norms $x \cdot y$ in the framework of quantum computation with mixed states. Note that the interval $[0, 1]$ equipped with the operations $\langle \oplus, \cdot, \neg \rangle$ defines an algebraic structure called *product MV-algebra* (PMV-algebra for short) [6, 19].

As an advantage of this probabilistic type representation, we can mathematically deal with circuits made from ensemble of Toffoli gates as $\langle \oplus, \cdot, \neg \rangle$-polynomial expressions in a PMV-algebra. In this way, PMV-algebra structure related to Toffoli gates plays a similar role to Boolean algebras describing digital circuits.

The paper is organized as follows: In Section 1, we introduce basic notions of quantum computation and we fix some mathematical notation. Section 2 contains generalities about tensor product structures to describe bipartite quantum systems. In Section 3, we provide a probabilistic-type representation for Toffoli gates based on product and Łukasiewicz $t$-norms. In Section 4, we study this representation for nonfactorized states. In Section 5, we apply the results obtained in an abstract way to two concrete examples. Finally, Section 6 is devoted to the conclusions.

## 1. Basic notions

In quantum computation, information is elaborated and processed by means of quantum systems. Pure states of a quantum system are described by unit vectors in a Hilbert space. A *quantum bit* or *qubit*, the fundamental concept of quantum computation, is a pure state in the Hilbert space $\mathbb{C}^2$. The *standard orthonormal basis* $\{|0\rangle, |1\rangle\}$ of $\mathbb{C}^2$ is generally called *quantum computational basis*. Intuitively, $|1\rangle$ is related to the truth logical value and $|0\rangle$ to the falsity. Thus, pure states $|\psi\rangle$ in $\mathbb{C}^2$ are superpositions of the basis vectors with complex coefficients $|\psi\rangle = c_0|0\rangle + c_1|1\rangle$ where $|c_0|^2 + |c_1|^2 = 1$.

In the usual representation of quantum computational processes, a quantum circuit is identified with an appropriate composition of *quantum gates*, mathematically represented by *unitary operators* acting on pure states of a convenient ($n$-fold tensor product) Hilbert space $\otimes^n \mathbb{C}^2$ [21]. A special basis, called the $2^n$-*standard orthonormal basis*, is chosen for $\otimes^n \mathbb{C}^2$. More precisely, it consists of the $2^n$-orthogonal states $|\iota\rangle$, $0 \leq \iota \leq 2^n$, where $\iota$ is in binary representation and $|\iota\rangle$ can be seen as the tensor product of states $|\iota\rangle = |\iota_1\rangle \otimes |\iota_2\rangle \otimes \ldots \otimes |\iota_n\rangle$, where $\iota_j \in \{0, 1\}$. It provides the standard quantum computational model, based on qubits and unitary operators.

In general, a quantum system is not in a pure state. This may be caused, for example, by the noncomplete efficiency in the preparation procedure or by the fact that systems cannot be completely isolated from the environment, undergoing decoherence of their states. On the other hand, there are interesting processes that cannot be encoded in unitary evolutions. For example, at the end of the computation a nonunitary operation—a measurement—is applied, and the state becomes a probability distribution over pure states, or what is called a *mixed state*. In view of these facts, several authors [1,3,4,7–10] have paid attention to a more general model of quantum computational processes where pure states are replaced by mixed states. In what follows we give a short description of this mathematical model.

To each vector of the quantum computational basis of $\mathbb{C}^2$ we may associate two density operators $P_0 = |0\rangle\langle 0|$ and $P_1 = |1\rangle\langle 1|$ that represent the standard basis in this framework. Let $P_1^{(2^n)}$ be the operator $P_1^{(2^n)} = (\otimes^{n-1} I) \otimes P_1$ on $\otimes^n \mathbb{C}^2$ where $I$ is the $2 \times 2$ identity matrix. Clearly, $P_1^{(2^n)}$ is a $2^n$-square matrix. By applying the Born rule, we consider the probability of a density operator $\rho$ as follows,

$$p(\rho) = \operatorname{tr}(P_1^{(2^n)} \rho).$$

We focus our attention on these probability values since it allows us to establish a link between Toffoli gate and fuzzy connectives. Note that, in the particular case in which $\rho = |\psi\rangle\langle\psi|$, where $|\psi\rangle = c_0|0\rangle + c_1|1\rangle$, we obtain $p(\rho) = |c_1|^2$. Thus, this probability value associated to $\rho$ is the generalization, in this model, of the probability that a measurement over $|\psi\rangle$ yields $|1\rangle$ as the output. A *quantum operation* [16] is a linear operator $\mathcal{E} : \mathcal{L}(H_1) \to \mathcal{L}(H_2)$ where $\mathcal{L}(H_i)$ is the space of linear operators in the complex Hilbert space $H_i$ $(i = 1, 2)$, representable as $\mathcal{E}(\rho) = \sum_i A_i \rho A_i^\dagger$, where $A_i$ are operators satisfying $\sum_i A_i^\dagger A_i = I$ (Kraus representation [16]). It can be seen that a quantum operation maps density operators into density operators. Each unitary operator $U$ gives rise to a quantum operation $\mathcal{O}_\mathcal{U}$ such that $\mathcal{O}_\mathcal{U}(\rho) = \mathcal{U}\rho\mathcal{U}^\dagger$ for any density operator $\rho$. The new model based on density operators and quantum operations is called *quantum computation with mixed states*. It allows us to represent irreversible processes as measurements in the middle of the computation.

## 2. Density operators on $n$-dimensional Hilbert spaces

Due to the fact that the Pauli matrices

$$\sigma_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \qquad \sigma_2 = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \qquad \sigma_3 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

and $I$ are a basis for the set of operators over $\mathbb{C}^2$, an arbitrary density operator $\rho$ over $\mathbb{C}^2$ may be represented as

$$\rho = \frac{1}{2}(I + s_1\sigma_1 + s_2\sigma_2 + s_3\sigma_3)$$

where $s_1, s_2$ and $s_3$ are three real numbers such $s_1^2 + s_2^2 + s_3^2 \leq 1$. The triple $(s_1, s_2, s_3)$ represents the point of the Bloch sphere that is uniquely associated to $\rho$. A similar canonical representation can be obtained for any $n$-dimensional Hilbert space by using the notion of generalized Pauli matrices.

DEFINITION 2.1. Let $\mathcal{H}$ be an $n$-dimensional Hilbert space and $\{|\psi_1\rangle, \ldots, |\psi_n\rangle\}$ be the canonical othonormal basis of $\mathcal{H}$. Let $k$ and $j$ be two natural numbers such that $1 \leq k < j \leq n$. Then, the *generalized Pauli matrices* are defined as

$$
\begin{aligned}
{}^{(n)}\sigma_1^{[k,j]} &= |\psi_j\rangle\langle\psi_k| + |\psi_k\rangle\langle\psi_j|, \\
{}^{(n)}\sigma_2^{[k,j]} &= i(|\psi_j\rangle\langle\psi_k| - |\psi_k\rangle\langle\psi_j|),
\end{aligned}
$$

and for $1 \leq k \leq n-1$,

$$
{}^{(n)}\sigma_3^{[k]} = \sqrt{\frac{2}{k(k+1)}}(|\psi_1\rangle\langle\psi_1| + \cdots + |\psi_k\rangle\langle\psi_k| - k|\psi_{k+1}\rangle\langle\psi_{k+1}|).
$$

Let $\mathcal{H}$ be an $n$-dimensional Hilbert space and $\{|\psi_1\rangle, \ldots, |\psi_n\rangle\}$ be the canonical orthonormal basis of $\mathcal{H}$. For a technical reason we introduce the following sets:

$$
\begin{aligned}
{}^{(n)}\mathfrak{P}_1 &= \{{}^{(n)}\sigma_1^{[k,j]} : 1 \leq k < j \leq n\}, \\
{}^{(n)}\mathfrak{P}_2 &= \{{}^{(n)}\sigma_2^{[k,j]} : 1 \leq k < j \leq n\}, \\
{}^{(n)}\mathfrak{P}_3 &= \{{}^{(n)}\sigma_2^{[k]} : 1 \leq k \leq n-1\}.
\end{aligned}
$$

One can see that ${}^{(n)}\mathfrak{P}_1$ and ${}^{(n)}\mathfrak{P}_2$ contain $n(n-1)/2$ matrices, while ${}^{(n)}\mathfrak{P}_3$ contains $n-1$ matrices. Thus, if we consider the set ${}^{(n)}\mathfrak{P} ={}^{(n)} \mathfrak{P}_1 \cup^{(n)} \mathfrak{P}_2 \cup^{(n)} \mathfrak{P}_3$, it contains $n^2-1$ matrices. For the sake of simplicity, we consider the set ${}^{(n)}\mathfrak{P}$ ordered as follows,

$$
{}^{(n)}\mathfrak{P} = \{\underbrace{\sigma_1, \ldots, \sigma_{\frac{n(n-1)}{2}}}_{{}^{(n)}\mathfrak{P}_1} \mid \underbrace{\sigma_{\frac{n(n-1)}{2}+1}, \ldots, \sigma_{n(n-1)}}_{{}^{(n)}\mathfrak{P}_2} \mid \underbrace{\sigma_{n(n-1)+1}, \ldots, \sigma_{n^2-1}}_{{}^{(n)}\mathfrak{P}_3}\}.
$$

If $\mathcal{H} = \mathbb{C}^2$, one immediately obtains

$$
\begin{aligned}
{}^{(2)}\sigma_1^{[1,2]} &= |0\rangle\langle 1| + |1\rangle\langle 0| = \sigma_1 && \text{and} && {}^{(2)}\mathfrak{P}_1 = \{\sigma_1\}, \\
{}^{(2)}\sigma_2^{[1,2]} &= i(|0\rangle\langle 1| - |1\rangle\langle 0|) = \sigma_2 && \text{and} && {}^{(2)}\mathfrak{P}_2 = \{\sigma_2\}, \\
{}^{(2)}\sigma_3^{[1]} &= |0\rangle\langle 0| - |1\rangle\langle 1| = \sigma_3 && \text{and} && {}^{(2)}\mathfrak{P}_3 = \{\sigma_3\}.
\end{aligned}
$$

As another example, if $n = 3$ we obtain the well-known *Gell-Mann matrices*.

LEMMA 2.1. *Let $\mathcal{H}$ be an n-dimensional Hilbert space and let $\{|\psi_j\rangle\}_{j=1}^n$ be an orthonormal basis of $\mathcal{H}$. For any $\sigma_j \in^{(n)} \mathfrak{P}$ such that $1 \leq j \leq n(n-1)$, i.e. $\sigma_j \in {}^{(n)}\mathfrak{P}_1 \cup {}^{(n)}\mathfrak{P}_2$, each diagonal element of $\sigma_j$ is* 0.

*Proof*: It follows from the fact that, if $k \neq j$ and $|\psi_j\rangle = (x_s^j)_{1\leq s\leq n}$, $|\psi_k\rangle = (x_s^k)_{1\leq s\leq n}$ then $\mathrm{diag}|\psi_k\rangle\langle\psi_j| = (x_s^j x_s^k)_{1\leq s\leq n}$. □

Let $\rho$ be a density operator of the $n$-dimensional Hilbert space $\mathcal{H}$. For any $j$ where $1 \leq j \leq n^2 - 1$, let

$$
s_j(\rho) = \mathrm{tr}(\rho\sigma_j).
$$

The sequence $\langle s_1(\rho) \ldots s_{n^2-1}(\rho)\rangle$ is called the *generalized Bloch vector* associated to $\rho$, in view of the following well-known result.

THEOREM 2.1. *Let $\rho$ be a density operator of the $n$-dimensional Hilbert space $\mathcal{H}$ and let $\sigma_j \in \mathfrak{P}_n$. Then $\rho$ can be canonically represented as follows,*

$$\rho = \frac{1}{n} I^{(n)} + \frac{1}{2} \sum_{j=1}^{n^2-1} s_j(\rho)\sigma_j,$$

*where $I^{(n)}$ is the $n \times n$ identity matrix.* □

A kind of converse of Theorem 2.1 reads: a matrix $\rho$ having the form $\rho = \frac{1}{n} I^{(n)} + \frac{1}{2} \sum_{j=1}^{n^2-1} s_j\sigma_j$ is a density operator iff all its eigenvalues are nonnegative.

Let us consider the Hilbert space $\mathcal{H} = \mathcal{H}_a \otimes \mathcal{H}_b$. For any density operator $\rho$ on $\mathcal{H}$, we denote by $\rho_a$ the partial trace of $\rho$ with respect to the system $\mathcal{H}_b$ (i.e. $\rho_a = \mathrm{tr}_{\mathcal{H}_b}(\rho)$) and by $\rho_b$ the partial trace of $\rho$ with respect to the system $\mathcal{H}_a$ (i.e. $\rho_b = \mathrm{tr}_{\mathcal{H}_a}(\rho)$). For the following developments it is useful to recall the next technical result.

LEMMA 2.2. *Let $\rho$ be a density operator in a Hilbert space $\mathcal{H} = \mathcal{H}_a \otimes \mathcal{H}_b$, where $\dim(\mathcal{H}_a) = m$ and $\dim(\mathcal{H}_b) = k$. If we divide $\rho$ in $m \times m$ blocks $B_{i,j}$, each of them is a $k$-square matrix, then*

$$\rho_a = \mathrm{tr}_{\mathcal{H}_b}(\rho) = \begin{bmatrix} \mathrm{tr}B_{1,1} & \mathrm{tr}B_{1,2} & \ldots & \mathrm{tr}B_{1,m} \\ \mathrm{tr}B_{2,1} & \mathrm{tr}B_{2,2} & \ldots & \mathrm{tr}B_{2,m} \\ \vdots & \vdots & \vdots & \vdots \\ \mathrm{tr}B_{m,1} & \mathrm{tr}B_{m,2} & \ldots & \mathrm{tr}B_{m,m} \end{bmatrix},$$

$$\rho_b = \mathrm{tr}_{\mathcal{H}_a}(\rho) = \sum_{i=1}^{m} B_{i,i}.$$

*Proof*: Let $\alpha$ be a density operator in $\mathcal{H}_a$ and $\beta$ be a density operator in $\mathcal{H}_b$. Then,

$$\alpha \otimes \beta = \begin{bmatrix} \alpha_{1,1}\beta & \alpha_{1,2}\beta & \ldots & \alpha_{1,m}\beta \\ \alpha_{2,1}\beta & \alpha_{2,2}\beta & \ldots & \alpha_{2,m}\beta \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_{m,1}\beta & \alpha_{m,2}\beta & \ldots & \alpha_{m,m}\beta \end{bmatrix}$$

$$= \begin{bmatrix} B_{1,1} & B_{1,2} & \dots & B_{1,m} \\ B_{2,1} & B_{2,2} & \dots & B_{2,m} \\ \vdots & \vdots & \vdots & \vdots \\ B_{m,1} & B_{m,2} & \dots & B_{m,m} \end{bmatrix},$$

where each $B_{i,j}$ entry is a $k$-square matrix. Since $\mathrm{tr}(\alpha) = \mathrm{tr}(\beta) = 1$, by definition of partial trace, we have that

$$\mathrm{tr}_{\mathcal{H}_b}(\alpha \otimes \beta) = \mathrm{tr}(\beta)\alpha = \begin{bmatrix} \mathrm{tr}B_{1,1} & \mathrm{tr}B_{1,2} & \dots & \mathrm{tr}B_{1,m} \\ \mathrm{tr}B_{2,1} & \mathrm{tr}B_{2,2} & \dots & \mathrm{tr}B_{2,m} \\ \vdots & \vdots & \vdots & \vdots \\ \mathrm{tr}B_{m,1} & \mathrm{tr}B_{m,2} & \dots & \mathrm{tr}B_{m,m} \end{bmatrix} = \alpha,$$

$$\mathrm{tr}_{\mathcal{H}_a}(\alpha \otimes \beta) = \mathrm{tr}(\alpha)\beta = \sum_{i=1}^{m} B_{i,i} = \beta.$$

These matrix representation of the reduced states combined with linearity, enables one to compute in practice all partial traces. In fact, for each density operator $\rho$ in $\mathcal{H}_a \otimes \mathcal{H}_b$, we have to consider the spectral decomposition of $\rho$ given by $\rho = \sum_{j,l} \sum_{s,n} \langle \psi_j \otimes \varphi_l | \rho \phi_s \otimes \varphi_n \rangle |\psi_j\rangle\langle\psi_s| \otimes |\varphi_l\rangle\langle\varphi_n|$ where $\{|\psi_j\rangle\}$ and $\{|\varphi_n\rangle\}$ are orthonormal bases for $\mathcal{H}_a$ and $\mathcal{H}_b$, respectively. Thus, the matrix representation for $\rho_a$ and $\rho_b$ follows immediately. □

DEFINITION 2.2. Let $\rho$ be a density operator in a Hilbert space $\mathcal{H}_m \otimes \mathcal{H}_k$ such that $\dim(\mathcal{H}_m) = m$ and $\dim(\mathcal{H}_k) = k$. Then $\rho$ is said to be *$(m, k)$-factorizable* iff $\rho = \rho_m \otimes \rho_k$, where $\rho_m$ is a density operator in $\mathcal{H}_m$ and $\rho_k$ is a density operator in $\mathcal{H}_k$.

It is well known that, if $\rho$ is $(m, k)$-factorizable as $\rho = \rho_m \otimes \rho_k$, this factorization is unique and $\rho_m$ and $\rho_k$ correspond to the reduced state of $\rho$ on $\mathcal{H}_m$ and $\mathcal{H}_k$, respectively.

Suppose that $\mathcal{H} = \mathcal{H}_a \otimes \mathcal{H}_b$, where $\dim(\mathcal{H}_a) = m$ and $\dim(\mathcal{H}_b) = k$. Consider the generalized Pauli matrices $\sigma_1^a \dots \sigma_{m^2-1}^a$ and $\sigma_1^b \dots \sigma_{k^2-1}^b$ arising from $\mathcal{H}_a$ and $\mathcal{H}_b$, respectively. Each density operator $\rho$ in $\mathcal{H}$ can be written as follows [22]

$$\rho = \frac{1}{mk} I^{(mk)} + \frac{1}{2m} \sum_{j=1}^{m^2-1} \mathrm{tr}(\rho[\sigma_j^a \otimes I^{(k)}])(\sigma_j^a \otimes I^{(k)})$$
$$+ \frac{1}{2k} \sum_{l=1}^{k^2-1} \mathrm{tr}(\rho[I^{(m)} \otimes \sigma_l^b])(I^{(m)} \otimes \sigma_l^b)$$

$$+\frac{1}{4}\sum_{j=1}^{m^2-1}\sum_{l=1}^{k^2-1}\operatorname{tr}(\rho[\sigma_j^a\otimes\sigma_l^b])(\sigma_j^a\otimes\sigma_l^b).$$

Now, let us consider the reduced states $\rho_a$ and $\rho_b$. Taking into account that $\operatorname{tr}(\rho[\sigma_j^a\otimes I^{(k)}])=\operatorname{tr}(\rho_a\sigma_j^a)$ and $\operatorname{tr}(\rho[I^{(m)}\otimes\sigma_l^b])=\operatorname{tr}(\rho_b\sigma_l^b)$, we can see that

$$\rho_a=\frac{1}{m}I^{(m)}+\frac{1}{2}\sum_{j=1}^{m^2-1}\operatorname{tr}(\rho[\sigma_j^a\otimes I^{(k)}])\sigma_j^a,$$

$$\rho_b=\frac{1}{k}I^{(k)}+\frac{1}{2}\sum_{l=1}^{k^2-1}\operatorname{tr}(\rho[I^{(m)}\otimes\sigma_l^b])\sigma_l^b,$$

and then

$$\rho-(\rho_a\otimes\rho_b)=\frac{1}{4}\sum_{j=1}^{m^2-1}\sum_{l=1}^{k^2-1}[\operatorname{tr}(\rho[\sigma_j^a\otimes\sigma_l^b])-\operatorname{tr}(\rho[\sigma_j^a\otimes I^{(k)}])\operatorname{tr}(\rho[I^{(m)}\otimes\sigma_l^b])](\sigma_j^a\otimes\sigma_l^b).$$

Thus we define the following coefficients:

$$M_{j,l}(\rho)=\operatorname{tr}(\rho[\sigma_j^a\otimes\sigma_l^b])-\operatorname{tr}(\rho[\sigma_j^a\otimes I^{(k)}])\operatorname{tr}(\rho[I^{(m)}\otimes\sigma_l^b]).$$

On this basis, the matrix $\mathbf{M}(\rho)$ defined as

$$\mathbf{M}(\rho)=\frac{1}{4}\sum_{j=1}^{m^2-1}\sum_{l=1}^{k^2-1}M_{j,l}(\rho)(\sigma_j^a\otimes\sigma_l^b)$$

represents the additional component of $\rho$ when $\rho$ is nonfactorized in $\mathcal{H}_a\otimes\mathcal{H}_b$. Thus, we can establish the following proposition.

PROPOSITION 2.1. [22] *Let $\rho$ be a density operator in $\mathcal{H}=\mathcal{H}_a\otimes\mathcal{H}_b$. Then,*

$$\rho=\rho_a\otimes\rho_b+\mathbf{M}(\rho).$$

PROPOSITION 2.2. *Suppose that $\mathcal{H}=\mathcal{H}_a\otimes\mathcal{H}_b$, where $\dim(\mathcal{H})=2^n$, $\dim\mathcal{H}_a=m$ and $\dim\mathcal{H}_b=k$. Let us consider a density operator $\rho$ in $\mathcal{H}$. Then*

1. $\operatorname{tr}(P_1^{(m+k)}(\mathbf{M}(\rho)))=0$,
2. *if* $\dim\mathcal{H}_b=2$ *then* $p(\rho)=p(\rho_b)$.

*Proof*: 1) Let $\rho$ be a density operator in $\mathcal{H}$. If we divide $\rho$ in $m\times m$ blocks $B_{i,j}$ of dimension $k\times k$ then by Lemma 2.2 we have that

$$\rho_a\otimes\rho_b=\begin{bmatrix}\operatorname{tr}B_{1,1}\sum_{i=1}^m B_{i,i} & \operatorname{tr}B_{1,2}\sum_{i=1}^m B_{i,i} & \dots & \operatorname{tr}B_{1,m}\sum_{i=1}^m B_{i,i}\\ \operatorname{tr}B_{2,1}\sum_{i=1}^m B_{i,i} & \operatorname{tr}B_{2,2}\sum_{i=1}^m B_{i,i} & \dots & \operatorname{tr}B_{2,m}\sum_{i=1}^m B_{i,i}\\ \vdots & \vdots & \vdots & \vdots\\ \operatorname{tr}B_{m,1}\sum_{i=1}^m B_{i,i} & \operatorname{tr}B_{m,2}\sum_{i=1}^m B_{i,i} & \dots & \operatorname{tr}B_{m,m}\sum_{i=1}^m B_{i,i}\end{bmatrix}.$$

Note that

$$\begin{aligned}\mathrm{tr}(P_1(\rho_a \otimes \rho_b)) &= \mathrm{tr} B_{1,1} \sum_{i=1}^{m} \mathrm{tr} P_1 B_{i,i} + \cdots + \mathrm{tr} B_{m,m} \sum_{i=1}^{m} \mathrm{tr} P_1 B_{i,i} \\ &= p(\rho)\mathrm{tr}(\rho) = p(\rho).\end{aligned}$$

Hence, $p(\rho) = \mathrm{tr}(P_1^{(m+k)}(\rho_a \otimes \rho_b + \mathbf{M}(\rho))) = \mathrm{tr}(P_1^{(m+k)}(\rho_a \otimes \rho_b)) + \mathrm{tr}(P_1^{(m+k)}\mathbf{M}(\rho))$ $= p(\rho) + \mathrm{tr}(P_1^{(m+k)}\mathbf{M}(\rho))$, and then $\mathrm{tr}(P_1^{(m+k)}\mathbf{M}(\rho)) = 0$.

2) Suppose that $\rho = (r_{i,j})_{1 \le i,j \le 2^n}$. If $\dim \mathcal{H}_b = 2$, by Lemma 2.2 $\rho_b$ has the form

$$\rho_2 = \begin{bmatrix} 1 - \sum_{i=1}^{2^m} r_{2i,2i} & b^* \\ b & \sum_{i=1}^{2^m} r_{2i,2i} \end{bmatrix} = \begin{bmatrix} 1 - p(\rho) & b^* \\ b & p(\rho) \end{bmatrix}.$$

Hence, $p(\rho) = p(\rho_b)$. □

## 3. Fuzzy representation of Toffoli gate

The Toffoli gate, introduced by Tommaso Toffoli [24], is a universal reversible logic gate, which means that any classical reversible circuit can be built from the Toffoli gates. This gate has three input bits $(x, y, z)$ and three output bits. Two of the bits, $x$ and $y$, are control bits that are unaffected by the action of the gate. The third bit $z$ is the target bit that is flipped if and only if both control bits are set to 1, and otherwise is left alone. The application of the Toffoli gate to a set of three bits is dictated by

$$T(x, y, z) = (x, y, xy \widehat{+} z)$$

where $\widehat{+}$ is the sum modulo 2. The Toffoli gate can be used to reproduce the classical AND gate when $z = 0$ and the NAND gate when $z = 1$.

The Toffoli gate can also be implemented as a quantum logical gate by permuting computational basis vectors $|0\rangle, |1\rangle$ as in the classical case.

DEFINITION 3.1. For any natural numbers $m, n \ge 1$ and for any vectors of the standard orthonormal basis $|x\rangle = |x_1 \dots x_m\rangle \in \otimes^m \mathbb{C}^2$, $|y\rangle = |y_1 \dots y_n\rangle \in \otimes^k \mathbb{C}^2$ and $|z\rangle \in \mathbb{C}^2$, the*Toffoli quantum gate* $T^{(m,n,1)}$ (from now on, shortly, Toffoli gate) on $\otimes^{m+n+1}\mathbb{C}^2$ is defined as follows

$$T^{(m,n,1)}(|x\rangle \otimes |y\rangle \otimes |z\rangle) = |x\rangle \otimes |y\rangle \otimes |x_m y_n \widehat{+} z\rangle.$$

It is well known that $T^{(m,n,1)}$ is a unitary operator. The following proposition describes the matrix representation of $T^{(m,n,1)}$ that will be used in the next sections.

PROPOSITION 3.1. *For any natural number $m, n \ge 1$,*

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

$$= I^{(2^{m-1})} \otimes \left[\begin{array}{c|c} I^{(2^{n+1})} & \mathbf{0} \\ \hline \mathbf{0} & I^{(2^{n-1})} \otimes \mathrm{Xor} \end{array}\right]$$

*where*

$$\mathrm{Not} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad \textit{and} \qquad \mathrm{Xor} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

*Proof*: Suppose that $|x\rangle = |x_1, \ldots, x_m\rangle$, $|y\rangle = |y_1, \ldots, y_n\rangle$ and $|z\rangle$ are basic vectors in $\otimes^m \mathbb{C}^2$, $\otimes^n \mathbb{C}^2$ and $\mathbb{C}^2$, respectively. Then

$$\begin{aligned}
&(I^{(2^{m+n+1})} + P_1^{(2^m)} \otimes P_1^{(2^n)} \otimes (\mathrm{Not} - I))|x\rangle \otimes |y\rangle \otimes |z\rangle \\
&\qquad = |x\rangle \otimes |y\rangle \otimes |z\rangle + (P_1^{(2^m)} \otimes P_1^{(2^n)} \otimes (\mathrm{Not} - I))|x\rangle \otimes |y\rangle \otimes |z\rangle \\
&\qquad = |x\rangle \otimes |y\rangle \otimes |z\rangle + P_1^{(2^m)}|x\rangle \otimes P_1^{(2^n)}|y\rangle \otimes (\mathrm{Not} - I)|z\rangle.
\end{aligned}$$

We have to consider two possible cases:

If $|x\rangle = |x_1 \ldots x_{m-1}, 1\rangle$ and $|y\rangle = |y_1 \ldots y_{n-1}, 1\rangle$, then $P_1^{(2^m)}|x\rangle = |x\rangle$ and $P_1^{(2^n)}|y\rangle = |y\rangle$. Hence,

$$\begin{aligned}
|x\rangle \otimes |y\rangle \otimes |z\rangle + P_1^{(2^m)}|x\rangle \otimes P_1^{(2^n)}|y\rangle \otimes (\mathrm{Not} - I)|z\rangle &= |x\rangle \otimes |y\rangle \otimes \mathrm{Not}|z\rangle \\
&= |x\rangle \otimes |y\rangle \otimes |x_m y_n \oplus z\rangle.
\end{aligned}$$

If $|x\rangle = |x_1 \ldots x_{m-1}, 0\rangle$ or $|y\rangle = |y_1 \ldots y_{n-1}, 0\rangle$, then $P_1^{(2^m)}|x\rangle = \mathbf{0}$ or $P_1^{(2^n)}|y\rangle = \mathbf{0}$, respectively. Hence,

$$\begin{aligned}
|x\rangle \otimes |y\rangle \otimes |z\rangle + P_1^{(2^m)}|x\rangle \otimes P_1^{(2^n)}|y\rangle \otimes (\mathrm{Not} - I)|z\rangle &= |x\rangle \otimes |y\rangle \otimes |z\rangle + \mathbf{0} \\
&= |x\rangle \otimes |y\rangle \otimes |x_m y_n \oplus z\rangle.
\end{aligned}$$

Thus,

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

Note that $P_1^{(2^m)} \otimes P_1^{(2^n)}$ is a $2^{m+n}$-square matrix having $2^m$-blocks placed as follows,

$$P_1^{(2^m)} \otimes P_1^{(2^n)} = \begin{bmatrix} \mathbf{0}^{(2^n)} & & & & \\ & P_1^{(2^n)} & & & \\ & & \mathbf{0}^{(2^n)} & & \\ & & & \ddots & \\ & & & & P_1^{(2^n)} \end{bmatrix}.$$

Hence, the matrix $P_1^{(2^m)} \otimes P_1^{(2^n)} \otimes (\mathrm{Not} - I)$ is a $2^{m+n+1}$-matrix having $2^m$-blocks, placed as follows,

$$P_1^{(2^m)} \otimes P_1^{(2^n)} \otimes (\mathrm{Not} - I) = \begin{bmatrix} \mathbf{0}^{(2^{n+1})} & & & & \\ & B & & & \\ & & \mathbf{0}^{(2^{n+1})} & & \\ & & & \ddots & \\ & & & & B \end{bmatrix},$$

where $B$ is a $2^{n+1}$-matrix having $2^n$-blocks placed as

$$B = \begin{bmatrix} \mathbf{0}^2 & & & & \\ & \mathrm{Not} - I & & & \\ & & \mathbf{0}^2 & & \\ & & & \ddots & \\ & & & & \mathrm{Not} - I \end{bmatrix}.$$

Thus, it is not very hard to see that

$$I^{(m+n+1)} + P_1^{(m)} \otimes P_1^{(n)} \otimes (\mathrm{Not} - I) = I^{(m-1)} \otimes \left[\begin{array}{c|c} I^{(n+1)} & \mathbf{0} \\ \hline \mathbf{0} & I^{(n-1)} \otimes \mathrm{Xor} \end{array}\right].$$

Hence, our claim follows. □

Since $T^{(m,n,1)}$ is a unitary self-adjoint operator, it gives rise to the following quantum operation.

DEFINITION 3.2. For any density operator $\rho$ in $\otimes^{m+n+1}\mathbb{C}^2$, where $m, n \geq 1$, we define the *Toffoli quantum operation* $\mathbb{T}^{(m,n,1)}$ as follows,

$$\mathbb{T}^{(m,n,1)}(\rho) = T^{(m,n,1)} \rho T^{(m,n,1)}.$$

For the sake of simplicity, for any $2^{m+n+1}$-matrix $A$ in $\otimes^{m+n+1}\mathbb{C}^2$, $\mathbb{T}_p^{(m,n,1)}(A)$ denotes the matrix

$$\mathbb{T}_p^{(m,n,1)}(A) = P_1^{(2^{m+n+1})}(T^{(m,n,1)} A T^{(m,n,1)}).$$

PROPOSITION 3.2. [10] *Consider the quantum operation* $\mathbb{NOT}^{(2^m)}$ *such that for each density operator* $\rho$ *in* $\otimes^m\mathbb{C}^2$,

$$\mathbb{NOT}^{(2^m)}(\rho) = (I^{(2^{m-1})} \otimes \mathrm{Not})\rho(I^{(2^{m-1})} \otimes \mathrm{Not}).$$

*Then:*

1. $p(\mathbb{NOT}^{(2^m)}(\rho)) = 1 - p(\rho)$,
2. $\mathbb{T}^{(m,n,1)}(\rho \otimes P_1) = \mathbb{NOT}^{(2^{m+n+1})}\mathbb{T}^{(m,n,1)}(\rho \otimes P_0)$ *for each density operator* $\rho$ *in* $\otimes^{m+n}\mathbb{C}^2$. □

PROPOSITION 3.3. *Let* $\rho$ *be a density operator in* $\otimes^{m+n}\mathbb{C}^2$, *where* $m, n \geq 1$ *and* $\sigma$ *be a density operator in* $\mathbb{C}^2$. *Then*

$$p(\mathbb{T}^{(m,n,1)}(\rho \otimes \sigma)) = (1 - p(\sigma))p(\mathbb{T}^{(m,n,1)}(\rho \otimes P_0)) + p(\sigma)(1 - p(\mathbb{T}^{(m,n,1)}(\rho \otimes P_0)).$$

*Proof*: Suppose that $\sigma = \begin{pmatrix} 1-\alpha & b^* \\ b & \alpha \end{pmatrix}$. Then $p(\sigma) = \mathrm{tr}(P_1\sigma) = \alpha$. Note that $\sigma = (1 - p(\sigma))P_0 + p(\sigma)P_1 + B$ where $B = \begin{pmatrix} 0 & b^* \\ b & 0 \end{pmatrix}$. Thus, by Proposition 3.2-2, we have that

$$\begin{aligned} p(\mathbb{T}^{(m,n,1)}(\rho \otimes \sigma)) = {} & (1 - p(\sigma))p(\mathbb{T}^{(m,n,1)}(\rho \otimes P_0)) \\ & + p(\sigma)p(\mathbb{NOT}^{(2^{m+n+1})}\mathbb{T}^{(m,n,1)}(\rho \otimes P_0)) \\ & + \mathrm{tr}(\mathbb{T}_p^{(m,n,1)}(\rho \otimes B)). \end{aligned}$$

Note that $\mathrm{diag}(\mathbb{T}^{(m,n,1)}(\rho \otimes B)) = \{0, 0, \ldots, 0\}$. Then $\mathrm{tr}(\mathbb{T}_p^{(m,n,1)}(\rho \otimes B)) = 0$. By Proposition 3.2-1, $p(\mathbb{NOT}^{(2^{m+n+1})}\mathbb{T}^{(m,n,1)}(\rho \otimes P_0)) = 1 - p(\mathbb{T}^{(m,n,1)}(\rho \otimes P_0))$. Hence, the proposition is proved. □

The connection between Toffoli gates and continuous $t$-norms is given by the generic probability values $p(\mathbb{T}^{(m,n,1)}(\cdot \otimes \cdot \otimes \cdot))$. In fact, we shall see that $p(\mathbb{T}^{(m,n,1)}(\cdot \otimes \cdot \otimes \cdot))$ can be described in terms of the operations $\langle \oplus, \cdot, \neg \rangle$. This idea is formalized as follows.

The term $\langle \oplus, \cdot, \neg \rangle_n$-*polynomial expression* denotes a function $f : [0, 1]^n \to [0, 1]$ built only using the three operations $\langle \oplus, \cdot, \neg \rangle$ and $n$ variables.

DEFINITION 3.3. Let $\mathcal{E} : \mathcal{L}(\otimes^m\mathbb{C}^2) \to \mathcal{L}(\otimes^r\mathbb{C}^2)$ be a quantum operation. Then $\mathcal{E}$ is said to be $\langle \oplus, \cdot, \neg \rangle_n$-representable if and only if there exists a $\langle \oplus, \cdot, \neg \rangle_n$-*polynomial expression* $f : [0, 1]^n \to [0, 1]$ and natural numbers $k_1, \ldots, k_n$ satisfying $k_1 + \cdots + k_n = m$, such that

$$p(\mathcal{E}(\rho_1 \otimes \ldots \otimes \rho_n)) = f(p(\rho_1), \ldots, p(\rho_n)),$$

where $\rho_i$ is a density operator in $(\otimes^{k_i}\mathbb{C}^2)$.

THEOREM 3.1. *Let* $\rho_m$ *be a density operator in* $\otimes^m\mathbb{C}^2$, $\rho_n$ *be a density operator in* $\otimes^n\mathbb{C}^2$ *and* $\sigma$ *be a density operator in* $\mathbb{C}^2$. *Then*

$$p(\mathbb{T}^{(m,n,1)}(\rho_m \otimes \rho_n \otimes \sigma)) = (1 - p(\sigma))p(\rho_m)p(\rho_n) \oplus p(\sigma)(1 - p(\rho_m)p(\rho_n))$$

*and* $\mathbb{T}^{(m,n,1)}$ *is* $\langle \oplus, \cdot, \neg \rangle_3$-*representable by* $\neg z \cdot x \cdot y \oplus z \cdot \neg(x \cdot y)$.

*Proof*: We first prove that $p(\mathbb{T}^{(m,n,1)}(\rho_m \otimes \rho_n \otimes P_0)) = p(\rho_m)p(\rho_n)$. By Proposition 3.1 we have

$$\begin{aligned}
p(\mathbb{T}^{(m,n,1)}(\rho_m \otimes \rho_n \otimes P_0)) &= \mathrm{tr}(P_1^{(2^{m+n+1})}\mathbb{T}^{(m,n,1)}(\rho_m \otimes \rho_n \otimes P_0)) \\
&= \mathrm{tr}(P_1^{(2^{m+n+1})}(I^{(2^{m+n+1})}(\rho_m \otimes \rho_n \otimes P_0)I^{(2^{m+n+1})})) \\
&\quad + \mathrm{tr}[P_1^{(2^{m+n+1})}(P_1^{(2^m)} \otimes P_1^{(2^n)} \otimes (\mathrm{Not} - I)) \\
&\quad (\rho_m \otimes \rho_n \otimes P_0)(P_1^{(2^m)} \otimes P_1^{(2^n)} \otimes (\mathrm{Not} - I))].
\end{aligned}$$

On the one hand, it is not very hard to see that

$$\mathrm{tr}(P_1^{(2^{m+n+1})}(I^{(2^{m+n+1})}(\rho_m \otimes \rho_n \otimes P_0)I^{(2^{m+n+1})})) = 0.$$

On the other hand,

$$\begin{aligned}
&\mathrm{tr}[P_1^{(2^{m+n+1})}(P_1^{(2^m)} \otimes P_1^{(2^n)} \otimes (\mathrm{Not} - I))(\rho_m \otimes \rho_n \otimes P_0)(P_1^{(2^m)} \otimes P_1^{(2^n)} \otimes (\mathrm{Not} - I))] \\
&\quad = \mathrm{tr}[(I^{(2^m)} \otimes I^{(2^n)} \otimes P_1)(P_1^{(2^m)}\rho_m P_1^{(2^m)} \otimes P_1^{(2^n)}\rho_n P_1^{(2^n)} \otimes ((\mathrm{Not} - I)P_0(\mathrm{Not} - I)))] \\
&\quad = \mathrm{tr}(P_1^{(2^m)}\rho_m P_1^{(2^m)}) \cdot \mathrm{tr}(P_1^{(2^n)}\rho_n P_1^{(2^n)}) \cdot \mathrm{tr}(P_1(\mathrm{Not}P_0\mathrm{Not} - P_0)) = p(\rho_m) \cdot p(\rho_n) \cdot 1.
\end{aligned}$$

Thus, by Proposition 3.3,

$$p(\mathbb{T}^{(m,n,1)}(\rho_m \otimes \rho_n \otimes \sigma)) = (1 - p(\sigma))p(\rho_m)p(\rho_n) + p(\sigma)(1 - p(\rho_m)p(\rho_n)).$$

Since $0 \leq p(\mathbb{T}^{(m,n,1)}(\rho_m \otimes \rho_n \otimes \sigma)) \leq 1$, the sum $(1 - p(\sigma))p(\rho_m)p(\rho_n) + p(\sigma)(1 - p(\rho_m)p(\rho_n))$ is a Łukasiewicz sum. Therefore, we can write

$$p(\mathbb{T}^{(m,n,1)}(\rho_m \otimes \rho_n \otimes \sigma)) = \neg p(\sigma)p(\rho_m)p(\rho_n) \oplus p(\sigma)\neg(p(\rho_m)p(\rho_n))$$

and $\mathbb{T}^{(m,n,1)}$ is $\langle \oplus, \cdot, \neg \rangle_3$-representable by $\neg z \cdot x \cdot y \ \oplus \ z \cdot \neg(x \cdot y)$. □

REMARK 3.1. An immediate consequence of the above theorem is the fact that $\mathbb{T}^{(m,n,1)}(- \otimes - \otimes P_0)$ (as quantum operation $\mathcal{L}(\otimes^{m+n}\mathbb{C}^2) \to \mathcal{L}(\otimes^{m+n+1}\mathbb{C}^2)$) is $\langle \oplus, \cdot, \neg \rangle_2$-representable by the product $t$-norm $x \cdot y$.

## 4. Toffoli gate and nonfactorized states

In the definition of Toffoli gate $T^{(m,n,1)}$, the ideal case in which inputs are in a product of pure states $|x\rangle \otimes |y\rangle \otimes |z\rangle$ was considered. In this case, by Theorem 3.1, $\mathbb{T}^{(m,n,1)}$ can be described only using the language of PMV-algebras. However, quantum systems continuously interact with environment, building up correlations. Then, for a more realistic approach, we intend to consider the more general case where the input of $\mathbb{T}^{(m,n,1)}$ could also be a mixed state $\rho$ in $\otimes^{m+n+1}\mathbb{C}^2$. In this way, the $\langle \oplus, \cdot, \neg \rangle_3$-representation of $\mathbb{T}^{(m,n,1)}$ given in Theorem 3.1 undergoes changes. In this section we will study the $\langle \oplus, \cdot, \neg \rangle_3$-representation of $\mathbb{T}^{(m,n,1)}$ in this general case.

PROPOSITION 4.1. *Let $\rho$ be a density operator in $\otimes^{m+n}\mathbb{C}^2$ and let us consider the representation $\rho = \rho_m \otimes \rho_n + \mathbf{M}(\rho)$ given in Proposition 2.1. Then,*

$$\mathrm{tr}(\mathbb{T}_p^{(m,n,1)}(\mathbf{M}(\rho) \otimes P_1)) = -\mathrm{tr}(\mathbb{T}_p^{(m,n,1)}(\mathbf{M}(\rho) \otimes P_0)).$$

*Proof*: By Proposition 2.1 and Theorem 3.1, we have

$$p(\mathbb{T}^{(m,n,1)}(\rho \otimes P_0) = p(\rho_m)p(\rho_n) + \mathrm{tr}(\mathbb{T}_p^{(m,n,1)}(\mathbf{M}(\rho) \otimes P_0)),$$
$$p(\mathbb{T}^{(m,n,1)}(\rho \otimes P_1) = (1 - p(\rho_m)p(\rho_n)) + \mathrm{tr}(\mathbb{T}_p^{(m,n,1)}(\mathbf{M}(\rho) \otimes P_1)).$$

By Proposition 3.2, $p(\mathbb{T}^{(m,n,1)}(\rho \otimes P_1)) = 1 - p(\mathbb{T}^{(m,n,1)}(\rho \otimes P_0))$. Therefore,

$$\begin{aligned} -\mathrm{tr}(\mathbb{T}_p^{(m,n,1)}(\mathbf{M}(\rho) \otimes P_1)) &= 1 - p(\mathbb{T}^{(m,n,1)}(\rho \otimes P_1)) - p(\rho_m)p(\rho_n)) \\ &= p(\mathbb{T}^{(m,n,1)}(\rho \otimes P_0)) - p(\rho_m)p(\rho_n)) \\ &= \mathrm{tr}(\mathbb{T}_p^{(m,n,1)}(\mathbf{M}(\rho) \otimes P_0)). \end{aligned}$$ □

PROPOSITION 4.2. *Let $\rho$ be a density operator in $\otimes^{m+n+1}\mathbb{C}^2$. Let $\rho_{m+n}$ and $\rho_2$ be the reduced states of $\rho$ on $\otimes^{m+n}\mathbb{C}^2$ and $\mathbb{C}^2$, respectively. Then*

$$p(\mathbb{T}^{(m,n,1)}(\rho)) = p(\mathbb{T}^{(m,n,1)}(\rho_{m+n} \otimes \rho_2)).$$

*Proof*: By Proposition 2.1, let us consider the representation $\rho = \rho_{m+n} \otimes \rho_2 + \mathbf{M}(\rho)$. We first prove that $\mathrm{tr}(\mathbb{T}_p^{(m,n,1)}(\mathbf{M}(\rho))) = 0$. By Proposition 3.1 we have that

$$\mathbb{T}^{(m,n,1)}(\mathbf{M}(\rho)) = \mathbf{M}(\rho) + P_1^{(2^m)} \otimes P_1^{(2^n)} \otimes (\mathrm{Not} - I)\mathbf{M}(\rho)P_1^{(2^m)} \otimes P_1^{(2^n)} \otimes (\mathrm{Not} - I).$$

Then, by Proposition 2.2,

$$\begin{aligned} &\mathrm{tr}(\mathbb{T}_p^{(m,n,1)}(\mathbf{M}(\rho))) \\ &\quad = \mathrm{tr}(P_1^{2^{m+n+1}}(P_1^{(2^m)} \otimes P_1^{(2^n)} \otimes (\mathrm{Not} - I)\mathbf{M}(\rho)P_1^{(2^m)} \otimes P_1^{(2^n)} \otimes (\mathrm{Not} - I))). \end{aligned}$$

Note that

$$\mathbf{M}(\rho) = \frac{1}{4}\sum_{j=1}^{(m+n)^2-1}\sum_{k=1}^{3} M_{j,k}(\rho)(\sigma_j^a \otimes \sigma_k),$$

where $\sigma_k$ are the usual Pauli matrices. If $k \neq 3$, then $\mathrm{diag}(\sigma_j^a \otimes \sigma_k)$ has the form $(0, 0 \ldots, 0)$. Thus,

$$\mathrm{tr}(P_1^{2^{m+n+1}}(P_1^{(2^m)} \otimes P_1^{(2^n)} \otimes (\mathrm{Not} - I)\sigma_j^a \otimes \sigma_k P_1^{(2^m)} \otimes P_1^{(2^n)} \otimes (\mathrm{Not} - I))) = 0.$$

Note that $(\mathrm{Not} - I)\sigma_3(\mathrm{Not} - I) = \mathbf{0}$. Then

$$\begin{aligned} \mathbf{0} &= (P_1^{(2^m)} \otimes P_1^{(2^n)}\sigma_j^a P_1^{(2^m)} \otimes P_1^{(2^n)}) \otimes ((\mathrm{Not} - I)\sigma_3(\mathrm{Not} - I)) \\ &= (P_1^{(2^m)} \otimes P_1^{(2^n)} \otimes (\mathrm{Not} - I))(\sigma_j^a \otimes \sigma_3)(P_1^{(2^m)} \otimes P_1^{(2^n)} \otimes (\mathrm{Not} - I)). \end{aligned}$$

Therefore,

$$\mathrm{tr}(P_1^{2^{m+n+1}}(P_1^{(2^m)} \otimes P_1^{(2^n)} \otimes (\mathrm{Not} - I)\sigma_j^a \otimes \sigma_3 P_1^{(2^m)} \otimes P_1^{(2^n)} \otimes (\mathrm{Not} - I))) = 0.$$

It proves that

$$\mathrm{tr}(\mathbb{T}_p^{(m,n,1)}(\mathbf{M}(\rho))) = 0.$$

Hence,

$$\begin{aligned} p(\mathbb{T}^{(m,n,1)}(\rho)) &= p(\mathbb{T}^{(m,n,1)}(\rho_{m+n} \otimes \rho_2)) + \mathrm{tr}(\mathbb{T}_p^{(m,n,1)}(\mathbf{M}(\rho)) \\ &= p(\mathbb{T}^{(m,n,1)}(\rho_{m+n} \otimes \rho_2)) + 0. \end{aligned}$$ □

The above proposition says that, if we want to calculate a probability value $p(\mathbb{T}^{(m,n,1)}(\cdot))$, then we can assume that the argument of $\mathbb{T}^{(m,n,1)}$ has the form $\rho_{m+n} \otimes \sigma$, where $\rho_{m+n}$ is a density operator in $\otimes^{m+n}\mathbb{C}^2$ and $\sigma$ is a density operator in $\mathbb{C}^2$.

THEOREM 4.1. *Let $\rho$ be a density operator in $\otimes^{m+n}\mathbb{C}^2$, $\rho_m$ be the reduced state of $\rho$ on $\otimes^m\mathbb{C}^2$ and $\rho_n$ be the reduced state of $\rho$ on $\otimes^n\mathbb{C}^2$, respectively. Then*

$$\begin{aligned} p(\mathbb{T}^{(m,n,1)}(\rho \otimes \sigma)) = {} & p(\mathbb{T}^{(m,n,1)}(\rho_m \otimes \rho_n \otimes \sigma)) \\ & + (1 - 2p(\sigma))\mathrm{tr}(\mathbb{T}_p^{(m,n,1)}(\mathbf{M}(\rho) \otimes P_0)). \end{aligned}$$

*Proof*: By Proposition 2.1 we have

$$p(\mathbb{T}^{(m,n,1)}(\rho \otimes \sigma)) = p(\mathbb{T}^{(m,n,1)}(\rho_m \otimes \rho_n \otimes \sigma)) + \mathrm{tr}(\mathbb{T}_p^{(m,n,1)}(\mathbf{M}(\rho) \otimes \sigma).$$

By the same argument as used in the proof of Proposition 3.3 and taking into account Proposition 4.1, we can see that

$$\begin{aligned} \mathrm{tr}(\mathbb{T}_p^{(m,n,1)}(\mathbf{M}(\rho) \otimes \sigma) &= (1 - p(\sigma))\mathrm{tr}(\mathbb{T}_p^{(m,n,1)}(\mathbf{M}(\rho) \otimes P_0)) \\ &\quad + p(\sigma)\mathrm{tr}(\mathbb{T}_p^{(m,n,1)}(\mathbf{M}(\rho) \otimes P_1)) \\ &= (1 - p(\sigma))\mathrm{tr}(\mathbb{T}_p^{(m,n,1)}(\mathbf{M}(\rho) \otimes P_0)) \\ &\quad - p(\sigma)\mathrm{tr}(\mathbb{T}_p^{(m,n,1)}(\mathbf{M}(\rho) \otimes P_0)) \\ &= (1 - 2p(\sigma))\mathrm{tr}(\mathbb{T}_p^{(m,n,1)}(\mathbf{M}(\rho) \otimes P_0)). \end{aligned}$$

Hence, the theorem is proved. □

By Theorem 3.1, we have

$$p(\mathbb{T}^{(m,n,1)}(\rho_m \otimes \rho_n \otimes \sigma)) = (1 - p(\sigma))p(\rho_m)p(\rho_n) \oplus p(\sigma)(1 - p(\rho_m)p(\rho_n)).$$

Hence, the last theorem say that, if the input of $T^{(m,n,1)}$ has the form $\rho \otimes \sigma$, then $\mathbb{T}^{(m,n,1)}$ preserves $\langle \oplus, \cdot, \neg \rangle_3$-representation in terms of reduced states of $\rho$, and further adds the term depending on $\mathrm{tr}(\mathbb{T}_p^{(m,n,1)}(\mathbf{M}(\rho) \otimes P_0))$. We shall refer to $p(\mathbb{T}^{(m,n,1)}(\rho_m \otimes \rho_n \otimes \sigma))$ as the *fuzzy component of* $\mathbb{T}^{(m,n,1)}(\rho \otimes \sigma)$. It is clear that, if $\sigma$ is of the form $\sigma = \begin{bmatrix} \frac{1}{2} & b^* \\ b & \frac{1}{2} \end{bmatrix}$, then the term $(1-2p(\sigma))\mathrm{tr}(\mathbb{T}_p^{(m,n,1)}(\mathbf{M}(\rho)\otimes P_0))$ does not fall into the fuzzy component of $\mathbb{T}^{(m,n,1)}(\rho\otimes\sigma)$.

REMARK 4.1. Suppose that the input of $\mathbb{T}^{(m,n,1)}$ is a general density operator $\rho$ in $\otimes^{m+n+1}\mathbb{C}^2$. Then $p(\mathbb{T}^{(m,n,1)}(\rho))$ can be easily described as follows.

Let us consider the reduced states of $\rho$, $\rho_{m+n}$ on $\otimes^{m+n}\mathbb{C}^2$ and $\rho_2$ in $\mathbb{C}^2$. By Proposition 2.2-2, $\rho_2$ has the form

$$\rho_2 = \begin{bmatrix} 1-p(\rho) & b^* \\ b & p(\rho) \end{bmatrix}.$$

Hence, by Proposition 4.2 and Theorem 4.1,

$$\begin{aligned} p(\mathbb{T}^{(m,n,1)}(\rho) &= p(\mathbb{T}^{(m,n,1)}(\rho_{m+n}\otimes\rho_2)) \\ &\quad + (1-2p(\rho))\mathrm{tr}(\mathbb{T}_p^{(m,n,1)}(\mathbf{M}(\rho_{m+n})\otimes P_0)) \\ &= (1-p(\rho))p(\rho_m)p(\rho_n)\oplus p(\rho)(1-p(\rho_m)p(\rho_n)) \\ &\quad + (1-2p(\rho))\mathrm{tr}(\mathbb{T}_p^{(m,n,1)}(\mathbf{M}(\rho_{m+n})\otimes P_0)), \end{aligned}$$

where $\rho_m$ and $\rho_n$ are the reduced states of $\rho_{m+n}$ on $\otimes^m\mathbb{C}^2$ and $\otimes^n\mathbb{C}^2$, respectively.

The rest of the section is devoted to the estimation of the terms that appear in the expression of $p(\mathbb{T}^{(m,n,1)}(-))$.

DEFINITION 4.1. Let $\rho = (r_{i,j})_{1\le i,j\le 2^{m+n+1}}$ be a density operator in $\otimes^{m+n}\mathbb{C}^2$ divided in $2^m\times 2^m$ blocks $T_{i,j}$ where each of them is a $2^n$-square matrix. Then, the $(m,n)$*-Toffoli blocks of* $\rho$ are the diagonal blocks $(T_i = T_{i,i})_{1\le i\le 2^m}$ of $\rho$. Moreover, we introduce the following parameters:

- $\beta^{m,n}(\rho) = \sum_{j=1}^{2^m-1}\sum_{i=0}^{2^{n-1}-1} r_{(2i+1)+j2^n}$, i.e. the sum of the odd diagonal elements of the even $(m,n)$-Toffoli blocks $T_{2i}$ of $\rho$,
- $\gamma^{m,n}(\rho) = \sum_{j=0}^{2^m-2}\sum_{i=1}^{2^{n-1}} r_{2i+j2^n}$, the sum of the even diagonal elements of the odd $(m,n)$-Toffoli blocks $T_{2i+1}$ of $\rho$,
- $\delta^{m,n}(\rho) = \sum_{j=1}^{2^m-1}\sum_{i=1}^{2^{n-1}} r_{2i+j2^n}$, the sum of the odd diagonal elements of the odd $(m,n)$-Toffoli blocks $T_{2i+1}$ of $\rho$.

PROPOSITION 4.3. *Let us consider a density operator $\rho$ in $\otimes^{m+n}\mathbb{C}^2$ with $m,n\ge 1$ and let $r_i$ be the $i$-th diagonal element of $\rho$. Then, we have that*

$$p(\mathbb{T}^{(m,n,1)}(\rho\otimes P_0)) = \sum_{j=1}^{2^{m-1}}\sum_{i=1}^{2^{n-1}} r_{(2j-1)2^n+2i},$$

*i.e. $p(\mathbb{T}^{(m,n,1)}(\rho\otimes P_0))$ is the sum of the even diagonal elements of the even $(m,n)$-Toffoli blocks $T_{2i}$ of $\rho$.*

*Proof*: We first note that $\mathrm{diag}(\rho \otimes P_0)$ has the form

$$\{|\underbrace{r_1, 0, r_2, 0, \ldots r_{2^n}, 0}_{A_1}| \ldots |\underbrace{r_{(\alpha-1)2^n+1}, 0, \ldots r_{\alpha 2^n}, 0}_{A_\alpha}| \ldots |\underbrace{r_{(2^m-1)2^n+1}, 0, \ldots r_{2^{m+n}}, 0}_{A_{2^m}}|\}.$$

By Proposition 3.1, we have that the diagonal of $\mathbb{T}^{(m,n,1)}(\rho \otimes P_0)$ has the form $\{|\tilde{A}_1| \ldots |\tilde{A}_\alpha| \ldots |\tilde{A}_{2^m}|\}$, where $\tilde{A}_\alpha = A_\alpha$ if $\alpha$ is odd and, if $\alpha$ is even, then each block $\tilde{A}_\alpha$ takes the form

$$\tilde{A}_\alpha = \underbrace{r_{(\alpha-1)2^n+1}, 0}, \underbrace{0, r_{(\alpha-1)2^n+2}}, \underbrace{r_{(\alpha-1)2^n+3}, 0}, \ldots, \underbrace{r_{(\alpha-1)2^n+2^n-1}, 0}, \underbrace{0, r_{\alpha 2^n}}.$$

Thus,

$$\begin{aligned} p(\mathbb{T}^{(m,n,1)}(\rho \otimes P_0)) &= \mathrm{tr}(P_1^{(2^{m+n+1})}(\mathbb{T}^{(m,n,1)}(\rho \otimes P_0))) \\ &= \sum_{j=0}^{2^{m-1}-1} \mathrm{tr}(P_1^{(2^{n+1})} \tilde{A}_{2j+1}) + \sum_{j=1}^{2^{m-1}} \mathrm{tr}(P_1^{(2^{n+1})} \tilde{A}_{2j}) \\ &= 0 + \sum_{j=1}^{2^{m-1}} \mathrm{tr}(P_1^{(2^{n+1})} \tilde{A}_{2j}). \end{aligned}$$

If $\alpha$ is an even number, taking into account the form of $\tilde{A}_\alpha$, we have that $\mathrm{tr}(P_1^{(2^{n+1})} \tilde{A}_\alpha) = \sum_{i=1}^{2^{n-1}} r_{(\alpha-1)2^n+2i}$. Hence, we have that $p(\mathbb{T}^{(m,n,1)}(\rho \otimes P_0)) = \sum_{j=1}^{2^{m-1}} \sum_{i=1}^{2^{n-1}} r_{(2j-1)2^n+2i}$. □

PROPOSITION 4.4. *Let $\rho$ be a density operator in $\otimes^{m+n}\mathbb{C}^2$. Let $\rho_m$ be the reduced state of $\rho$ on $\otimes^m\mathbb{C}^2$ and let $\rho_n$ be the reduced state of $\rho$ on $\otimes^n\mathbb{C}^2$. Then,*

1. $p(\rho_m) = p(\mathbb{T}^{(m,n,1)}(\rho \otimes P_0)) + \beta^{m,n}(\rho)$,
2. $p(\rho_n) = p(\mathbb{T}^{(m,n,1)}(\rho \otimes P_0)) + \gamma^{m,n}(\rho)$,
3. $\mathrm{tr}(\mathbb{T}_p^{(m,n,1)}(\mathbf{M}(\rho) \otimes P_0)) = p(\mathbb{T}^{(m,n,1)}(\rho \otimes P_0))\delta^{m,n}(\rho) - \beta^{m,n}(\rho)\gamma^{m,n}(\rho)$.

*Proof*: Let us consider the $(m, n)-$Toffoli blocks $(T_i)_{1\leq i\leq 2^m}$ of $\rho$.

1) By Lemma 2.2, we have that $p(\rho_m) = \sum_{i=1}^{2^{m-1}} \mathrm{tr}(T_{2i})$. Note that this sum can be seen as the sum of the even and odd elements of even Toffoli blocks. Then, by Proposition 4.3 and Definition $\beta^{m,n}(\rho)$, follows our claim.

2) Follows by analogous arguments as used in 1).

3) Immediately follows from the items 1) and 2). □

## 5. Fuzzy component and nonfactorized states: two examples

By Proposition 4.4, we can see that, if the input of $\mathbb{T}^{(m,n,1)}$ is nonfactorized then

1. the terms $p(\sigma)$, $p(\rho_m)$ and $p(\rho_n)$ in the fuzzy component $(1-p(\sigma))p(\rho_m)p(\rho_n) \oplus p(\sigma)(1 - p(\rho_m)p(\rho_n))$ are dependent one an another;

2. the term $\mathrm{tr}(\mathbb{T}_p^{(m,n,1)}(\mathbf{M}(\rho) \otimes P_0))$ is in addition to the fuzzy component.

In this section we study these cases in two concrete examples.

### 5.1. Dependent variables in the fuzzy component of $\mathbb{T}^{(1,1,1)}$

In this subsection we study the fuzzy component of $\mathbb{T}^{(1,1,1)}$ in the particular case in which $\mathrm{tr}(\mathbb{T}_p^{(1,1,1)}(\mathbf{M}(-) \otimes P_0)) = 0$. Let us consider the case $\mathbb{T}^{(1,1,1)}(\rho \otimes P_0)$ where $\rho$ is a density operator in $\mathbb{C}^2 \otimes \mathbb{C}^2$. The $(1,1)$-Toffoli blocks of $\rho$ have the general form

$$\rho = \left[\begin{array}{c|c} T_1 & \\ \hline & T_2 \end{array}\right] = \left[\begin{array}{cc|cc} d & & & \\ & c & & \\ \hline & & b & \\ & & & a \end{array}\right].$$

By Proposition 4.3, we have that $p(\mathbb{T}^{(1,1,1)}(\rho \otimes P_0)) = a$ and, by Proposition 4.4, $\mathrm{tr}(\mathbb{T}_p^{(1,1,1)}(\mathbf{M}(\rho) \otimes P_0)) = ad - bc$. Thus, if $ad = bc$, the quantity $\mathrm{tr}(\mathbb{T}_p^{(1,1,1)}(\mathbf{M}(\rho) \otimes P_0)) = 0$ and it has not any incidence in the fuzzy component of $\mathbb{T}^{(1,1,1)}(\rho \otimes P_0)$. Let us assume that $ad = bc$. Then

$$p(\mathbb{T}^{(1,1,1)}(\rho \otimes P_0)) = p(\rho_\alpha) \cdot p(\rho_\beta),$$

where $\rho_\alpha$ and $\rho_\beta$ are the reduced states of $\rho$. By Proposition 2.2, $p(\rho_\alpha) = b + a$ and $p(\rho_\beta) = c + a$. Therefore,

$$p(\mathbb{T}^{(1,1,1)}(\rho \otimes P_0)) = a = (a+b)(a+c). \tag{1}$$

Note that Eq. (1) is equivalent to the two following conditions,

$$a + b + c + d = 1, \qquad ad = bc. \tag{2}$$

It is not hard to see that

$$p(\mathbb{T}^{(1,1,1)}(\rho \otimes P_0)) = a = \frac{(1-b-c) \pm \sqrt{(1-b-c)^2 - 4bc}}{2}$$

where the two possible values of $a$ depend on the choice of $d$ in Eq. (2). More precisely,

$$d = 1 - \frac{(1-b-c) \pm \sqrt{(1-b-c)^2 - 4bc}}{2} - b - c.$$

Although the term $\mathrm{tr}(\mathbb{T}_p^{(1,1,1)}(\mathbf{M}(\rho) \otimes P_0)) = 0$, the fuzzy component of $\mathbb{T}^{(m,n,1)}$ is

$$p(\rho_\alpha)p(\rho_\beta) = \frac{(1-b-c) \pm \sqrt{(1-b-c)^2 - 4bc}}{2}.$$

Let us notice that, because of the nonfactorizablity of the imput state $\rho$, the quantities $p(\rho_\alpha)$ and $p(\rho_\beta)$ dependent each other, and then the fuzzy component does not faithfully correspond to the product $t$-norm.

### 5.2. Constant fuzzy component: Werner states

The Werner states provide an interesting example because they maintain a constant value of the fuzzy component of $\mathbb{T}^{(2^n,2^n,1)}(-\otimes P_0)$, regardless of the dimension of the state and of the degree of entanglement (see Proposition 5.3-2). In this way, it is possible to see the incidence of $\mathrm{tr}(\mathbb{T}_p^{(m,n,1)}(\mathbf{M}(-)\otimes P_0))$ in the fuzzy component. The Werner states, originally introduced in [25] for two particles to distinguish between the classical correlation and the fullfilment of Bell inequality are interesting for applications in quantum information theory. Examples of this are the entanglement teleportation via Werner states [17], the study of deterministic purification [23], etc.

DEFINITION 5.1. Let us consider a Hilbert space $\mathcal{H}\otimes\mathcal{H}$ such that $\dim\mathcal{H}=n$. A *Werner state* in $\mathcal{H}\otimes\mathcal{H}$ is a density operator $\rho$ such that, for any $n$-dimensional unitary operator $U$,

$$\rho=(U\otimes U)\rho(U^\dagger\otimes U^\dagger).$$

We can express Werner states as a linear combination of the identity and SWAP operators [14, § 6.4.3],

$$\rho=\rho_w^{(n^2)}=\frac{n+1-2w}{n(n^2-1)}I^{(n^2)}-\frac{n+1-2wn}{n(n^2-1)}\mathrm{SWAP}^{(n^2)}, \tag{3}$$

where $w\in[0,1]$ and $\mathrm{SWAP}^{(n^2)}=\sum_{i,j}|\psi_i\rangle\langle\psi_j|\otimes|\psi_j\rangle\langle\psi_i|$ with $|\psi_i\rangle$ and $|\psi_j\rangle$ vectors of the $n$-dimensional computational basis.

We first need to study some properties about the matrix representation of Werner states.

PROPOSITION 5.1. *Let us consider the Hilbert space* $\mathcal{H}\otimes\mathcal{H}$ *such that* $\dim(\mathcal{H})=n$. *Then* $\mathrm{SWAP}^{(n^2)}=(s_{k,l})_{1\le k,l\le n^2}$ *where*

$$s_{k,l}=\begin{cases}1, & k=(j-1)n+i,\ \ l=(i-1)n+j,\ \ 1\le j,i\le n,\\ 0, & otherwise.\end{cases}.$$

*Proof*: Let $|\psi_i\rangle_{1\le i\le n}$ be vectors of the $n$-dimensional basis of $\mathcal{H}$. Note that

$$\mathrm{SWAP}^{(n^2)}(|\psi_i\rangle\otimes|\psi_j\rangle)=|\psi_j\rangle\otimes|\psi_i\rangle. \tag{4}$$

In fact,

$$\begin{aligned}\mathrm{SWAP}^{(n^2)}(|\psi_i\rangle\otimes|\psi_j\rangle)&=\Big(\sum_{k,l}|\psi_k\rangle\langle\psi_l|\otimes|\psi_l\rangle\langle\psi_k|\Big)|\psi_i\rangle\otimes|\psi_j\rangle\\&=\sum_{k,l}|\psi_k\rangle\langle\psi_l|\psi_i\rangle\otimes|\psi_l\rangle\langle\psi_k|\psi_j\rangle\\&=|\psi_j\rangle\otimes|\psi_i\rangle.\end{aligned}$$

Suppose that $|\psi_i\rangle$ and $|\psi_j\rangle$ are the basis vectors in $\mathcal{H}$ such that their $i$-th and the $j$-th entries are equal to 1, respectively. Note that the vector $|\psi_i\rangle\otimes|\psi_j\rangle$ is a basis vector in $\mathcal{H}\otimes\mathcal{H}$ having 1 in the $(i-1)n+j$ -th entry, and by Eq. (4), $\mathrm{SWAP}^{(n^2)}(|\psi_i\rangle\otimes|\psi_j\rangle)$ is the basis vector in $\mathcal{H}\otimes\mathcal{H}$ having 1 in the $(j-1)n+i$ -th entry. Thus, $\mathrm{SWAP}^{(n^2)}$ moves the 1 from the $(i-1)n+j$ -th entry to the $(j-1)n+i$ -th entry, and leaves the other entries unchanged. Hence, our claim follows. □

PROPOSITION 5.2. *Let us consider a Werner state* $\rho_w^{(n^2)}=(r_{k,l})_{1\le k,l\le n^2}$. *Then*

$$r_{k,l}=\begin{cases} H=\dfrac{2w}{n(n+1)}, & k=l=(j-1)n+j,\ 1\le j\le n,\\ J=\dfrac{n+1-2w}{n(n^2-1)}, & k=l\neq(j-1)n+j,\ 1\le j\le n,\\ Q=\dfrac{2nw-n-1}{n(n^2-1)}, & k\neq l,\ k=(j-1)n+i,\ l=(i-1)n+j,\ 1\le j,\ i\le n,\\ 0 & otherwise\end{cases}$$

*In particular, the diagonal of* $\rho_w^{(n^2)}$ *has the following form*

$$\begin{aligned}&\mathrm{diag}(\rho_w^{(n^2)})\\&\quad=\{(H,\underbrace{J,\ldots,J),(J}_{n},H,\underbrace{J,\ldots,J),(J,J}_{n},H,J,\ldots,J),\ldots,\underbrace{J,(J\ldots,J}_{n},H)\}.\end{aligned}$$

*Proof*: It immediately follows from Proposition 5.1 and Eq. (3). □

PROPOSITION 5.3. *Let us consider a Werner state* $\rho_w^{(2^{2n})}$ *in* $\otimes^{n+n}\mathbb{C}^2$. *Then*

1. $p(\mathbb{T}^{(2^n,2^n,1)}(\rho_w^{(2^{2n})}\otimes P_0))=\dfrac{2^{2n}+2^n(2w-1)-2}{4(2^{2n}-1)}$,
2. $p(\rho_w^{(2^{2n})}{}_n)=\dfrac{1}{2}$ *where* $\rho_w^{(2^{2n})}{}_n$ *is the reduced state of* $\rho_w^{(2^{2n})}$ *on* $\otimes^n\mathbb{C}^2$,
3. $\mathrm{tr}(\mathbb{T}_p^{(2^n,2^n,1)}(\mathbf{M}(\rho_w^{(2^{2n})})\otimes P_0))=w2^{n+1}-2^n-1/4(2^{2n}-1)$.

*Proof*: By considering the $(2^n,2^n)$-Toffoli blocks of $\rho_w^{(2^{2n})}$ and by Proposition 5.2, we have that

$$\begin{aligned}&\mathrm{diag}(\rho_w^{(2^{2n})})\\&\quad=\{(H,\underbrace{J,\ldots,J),(J}_{2^n},H,\underbrace{J,\ldots,J),(J,J}_{2^n},H,J,\ldots,J),\ldots,\underbrace{J,(J\ldots,J}_{2^n},H)\},\end{aligned}$$

where each $j$-th $2^n$-tuple is the diagonal of the Toffoli block $T_j$. It is easy to see that the $j$-th $2^n$-tuple of $\mathrm{diag}(\rho_w^{(2^{2n})})$ contains one and only one $H$ in the $j$-th entry and $J$ in all other entries. Moreover, $H$ can be found in an even entry of every even $j$-th $2^n$-tuple ($j=2t$) and in an odd entry of every odd $j$-th $2^n$-tuple ($j=2t-1$).

1) The number of even $2^n$-tuple is $2^{n-1}$. Each of them has one $H$ in even entries and $2^{n-1}-1$ occurrences of $J$ in the rest of the even entries. Therefore, by Proposition 4.3,

$$p(\mathbb{T}^{(2^n,2^n,1)}(\rho_w^{(2^{2n})} \otimes P_0)) = 2^{n-1}[H + (2^{n-1}-1)J] = \frac{2^{2n} + 2^n(2w-1) - 2}{4(2^{2n}-1)}.$$

2) We first prove that

$$\beta^{(2^n,2^n)}(\rho_w^{(2^{2n})}) = \gamma^{(2^n,2^n)}(\rho_w^{(2^{2n})}) = \frac{2^{2n} + 2^n - 2^{n+1}w}{4(2^{2n}-1)}.$$

Each odd $2^n$-tuple has $J$ in all odd entries, since we have $2^{n-1}$ odd $2^n$-tuple

$$\beta^{(2^n,2^n)}(\rho_w^{(2^{2n})}) = 2^{2(n-1)}J = 2^{2(n-1)}\frac{2^n + 1 - 2w}{2^n(2^{2n}-1)} = \frac{2^{2n} + 2^n - 2^{n+1}w}{4(2^{2n}-1)}.$$

With the same argument we can prove that $\gamma^{(2^n,2^n)}(\rho_w^{(2^{2n})}) = 2^{2(n-1)}J$. Hence, by Proposition 4.4,

$$\begin{aligned} p(\rho_{w\ \ n}^{(2^{2n})}) &= p(\mathbb{T}^{(2^n,2^n,1)}(\rho_w^{(2^{2n})} \otimes P_0)) + \beta^{(2^n,2^n)}(\rho_w^{(2^{2n})}) \\ &= \frac{2^{2n} + 2^n(2w-1) - 2}{4(2^{2n}-1)} + \frac{2^{2n} + 2^n - 2^{n+1}w}{4(2^{2n}-1)} = \frac{1}{2}. \end{aligned}$$

3) Immediate from the items 1 and 2. □

The fuzzy component of $\mathbb{T}^{(2^n,2^n,1)}(\rho_w^{(2^{2n})} \otimes P_0)$ is $\frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$. Therefore,

$$p(\mathbb{T}^{(2^n,2^n,1)}(\rho_w^{(2^{2n})} \otimes P_0)) = \frac{1}{4} + \frac{w2^{n+1} - 2^n - 1}{4(2^{2n}-1)}.$$

Note that, $w = \frac{2^n + 1}{2^{n+1}}$ iff $\frac{w2^{n+1} - 2^n - 1}{4(2^{2n}-1)} = 0$ iff $\rho_w^{(2^{2n})} = \frac{1}{2^{2n}} I^{(2^{2n})}$ i.e. the Werner state is factorized.

Fig. 1 allows us to see the incidence of $\mathrm{tr}(\mathbb{T}_p^{(2^n,2^n,1)}(\mathbf{M}(\rho_w^{(2^{2n})}) \otimes P_0))$ on $p(\mathbb{T}^{(2^n,2^n,1)}(\rho_w^{(2^{2n})} \otimes P_0))$ for $w \in [0,1]$ and $n = 1,2,3$. When the dimension of the space $\otimes^{n+n}\mathbb{C}^2$ is large enough, the incidence of $\mathrm{tr}(\mathbb{T}_p^{(2^n,2^n,1)}(\mathbf{M}(\rho_w^{(2^{2n})}) \otimes P_0))$ on $p(\mathbb{T}^{(2^n,2^n,1)}(\rho_w^{(2^{2n})} \otimes P_0))$ tends to disappear and $p(\mathbb{T}^{(2^n,2^n,1)}(\rho_w^{(2^{2n})} \otimes P_0)) \approx \frac{1}{4}$, which is the fuzzy component.

## 6. Conclusions

In this paper we have introduced and studied a probabilistic type representation for the Toffoli gate. This representation establishes a relation between the mentioned gate and two continuous $t$-norms: Łukasiewicz and product $t$-norms. An algebraic structure that jointly encodes these $t$-norms is known as PMV-algebra. In this way,

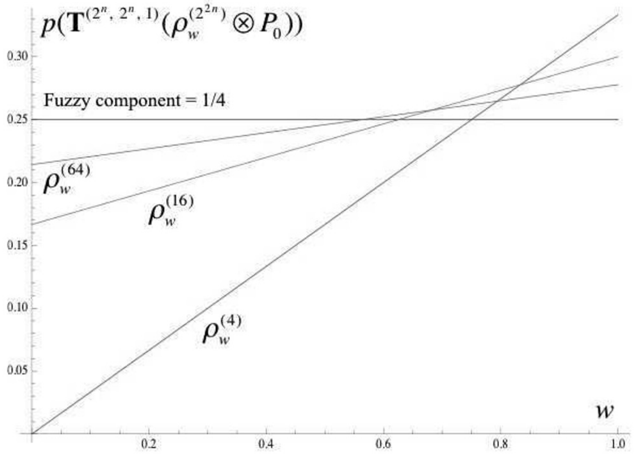


**Fig. 1.** Fuzzy component vs. incidence of $\mathrm{tr}(\mathbb{T}_p^{(2^n,2^n,1)}(\mathbf{M}(\rho_w^{(2^{2n})}) \otimes P_0))$.

we can mathematically represent ensemble of Toffoli gates by using term operation in a PMV-algebra.

However, this representation is interesting not only for its relation with PMV-algebras. In fact, Łukasiewicz and product $t$-norms are also known for their relations with game theory applied to the theory of communication with feedback. For example, the Łukasiewicz $t$-norm is related to Ulam's games [20] and the product $t$-norm is specially applied in fuzzy control [5] and allows us to model a probabilistic variant of Ulam's game: the so-called Pelc's game [18]. It could also suggest further developments as possible applications to the study of error-correcting codes in the context of quantum computation.

## Acknowledgements

The authors wish to thank anonymous referees for their careful reading and valuable comments on an earlier draft of this article.

This work was partially supported by the following grants: PIP 112-201101-00636, CONICET-Argentina and FIRB project "Structures and dynamics of knowledge and cognition", Cagliari Unit F21J12000140001, Italian Ministry of Scientific Research.

REFERENCES

[1] D. Aharanov, A. Kitaev, N. Nisan: Quantum circuits with mixed states, *Proc. 13th Annual ACM Symp. on Theory of Computation*, STOC (1997), 20–30.

[2] G. Cattaneo, M. Dalla Chiara, R. Giuntini, R. Leporini: An unsharp logic from quantum computation, *Int. J. Theor. Phys.* **43** (2001), 1803–1817.

[3] M. L. Dalla Chiara, R. Giuntini, R. Greechie: *Reasoning in Quantum Theory, Sharp and Unsharp Quantum Logics*, Kluwer, Dordrecht-Boston-London 2004.

[4] G. Domenech, H. Freytes: Fuzzy propositional logic associated with quantum computational gates, *Int. J. Theor. Phys.* **34** (2006), 228–261.
[5] D. Driankov, H. Hellendoorn, M. Reinfrank: *An Introduction to Fuzzy Control*, Springer, Berlin/Heidelberg 1993.
[6] A. Di Nola, A. Dvurečenskij: Product MV-algebras, *Multi. Val. Logic* **6** (2001), 193–215.
[7] H. Freytes, G. Sergioli, A. Aricó: Representing continuous $t$-norms in quantum computation with mixed states, *J. Phys. A* **43** (2010), 465306.
[8] H. Freytes., G. Domenech: Quantum computational logic with mixed states, *Mathematical Logic Quarterly* **59** (2013), 27–50.
[9] R. Giuntini, A. Ledda, G. Sergioli, F. Paoli: Some generalizations of fuzzy structures in quantum computational logic, *Int. J. Gen. Syst.* **40** (2011), 61–83.
[10] S. Gudder: Quantum computational logic, *Int. J. Theor. Phys.* **42** (2003), 39–47.
[11] S. Gudder, R. Greechie: Sequential products on effect algebras, *Rep. Math. Phys.* **49** (2002), 87–111.
[12] S. Gudder S, R. Greechie: Uniqueness and Order in Sequential Effect Algebras, *Int. J. Theor. Phys.* **44** (2005), 755-770.
[13] P. Hájek: *Metamathematics of Fuzzy Logic*, Trends in Logic Vol 4, Dordrecht, Kluwer 1998.
[14] T. Heinosaari, M. Ziman: *The Mathematical Language of Quantum Theory: From Uncertainty to Entanglement*, Cambridge University Press 2012.
[15] E. P. Klement, R. Mesiar, E. Pap, *Triangular norms*, Trends in Logic Vol. 8, Kluwer, Dordrecht 2000.
[16] K. Kraus: *States, Effects and Operations*, Springer, Berlin 1983.
[17] J. Lee, M.S. Kim: Entanglement Teleportation via Werner States, *Phys. Rev. Lett.* **84** (2000), 4236–4239.
[18] F. Montagna, C. Marini, G. Simi: Product logic and probabilistic Ulam games, *Fuzzy Sets and Systems* **158** (2007), 639–651.
[19] F. Montagna: Functorial representation theorems for $MV_\delta$ algebras with additional operators, *J. Algebra* **238** (2001), 99-125.
[20] D. Mundici: Ulam games, Łukasiewicz logic and AF $C^*$ algebras, *Fundam. Inform.* **18**, 151–61 (1993).
[21] A. M. Nielsen, I. L. Chuang: *Quantum Computation and Quantum Information*, Cambridge University Press 2000.
[22] J. Schlienz, G. Mahler: On the description of entanglement, *Phys. Rev. A* **52** (1995), 4396–4404.
[23] A. Short: No deterministic purification for two copies of a noisy entangled state, *Phys. Rev. Lett.* **102** (2009), 180502.
[24] T. Toffoli: Reversible computing, *Proceedings of the 7th Colloquium on Automata, Languages and Programming*, Springer London, UK, 632–644 (1980).
[25] R. F. Werner: Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model, *Phys. Rev. A* **40** (1989), 4277–4281.