

Applications of the Tracy-Singh product of matrices in quantum computation

Fabienne Chouraqui
Department of Exact sciences
University of Haifa at Oranim, Israel
fchoura@sci.haifa.ac.il

Abstract

The Tracy-Singh product of matrices is a generalisation of the Kronecker product of matrices, called sometimes the block Kronecker product, as it requires a partition of the matrices into blocks. In this paper, we give a survey on the applications of the Tracy-Singh product in several different domains, and in particular in quantum computing.

Keywords

Yang-Baxter Equation, Quantum entanglement, Tracy-Singh product of matrices

INTRODUCTION

The Kronecker product (or tensor product) of matrices is a fundamental concept in linear algebra and the Tracy-Singh product (TS) of matrices is a generalisation of it, called sometimes the block Kronecker product, as they share many properties. While the Kronecker product of two matrices has a very natural interpretation, indeed it represents the tensor product of the corresponding linear transformations, it is not known whether the TS has a general interpretation, and it is not much understood. In this paper, we give a survey on the Tracy-Singh product of matrices and on some of its recent applications in several domains, as the Yang-Baxter equation, and quantum computing. Furthermore, some connections have been established between the TS product and a categorical construction.

1 PRELIMINARIES ON THE TRACY-SINGH PRODUCT OF MATRICES AND ITS PROPERTIES

We refer to [10], [17], [18], [23], [22] for more details. Let $A = (a_{ij})$ be a matrix of size $m \times n$ and $B = (b_{kl})$ of size $p \times q$. Let $A = (A_{ij})$ be partitioned with A_{ij} of size $m_i \times n_j$ as the ij -th block submatrix and let $B = (B_{kl})$ be partitioned with B_{kl} of size $p_k \times q_l$ as the kl -th block submatrix ($\sum m_i = m, \sum n_j = n, \sum p_k = p, \sum q_l = q$). The Kronecker (or tensor) product and the Tracy-Singh (or block Kronecker) product are defined as follows:

1. The Kronecker (or tensor) product:

$$A \otimes B = (a_{ij}b_{kl})_{ij}$$

The matrix $A \otimes B$ is of size $mp \times nq$ and the block $a_{ij}b_{kl}$ is size $p \times q$.

2. The Tracy-Singh (or block Kronecker) product:

$$A \boxtimes B = ((A_{ij} \otimes B_{kl})_{kl})_{ij}$$

The matrix $A \boxtimes B$ is of size $mp \times nq$ and the block $A_{ij} \otimes B_{kl}$ is size $m_i p \times n_j q$. For non-partitioned matrices, $A \boxtimes B = A \otimes B$.

Example 1.1. We illustrate the Tracy-Singh product with A and B partitioned into blocks: $A \boxtimes B = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \boxtimes$

$$\begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix} = \begin{pmatrix} (1 \ 2) \otimes \begin{pmatrix} 5 \\ 7 \end{pmatrix} & (1 \ 2) \otimes \begin{pmatrix} 6 \\ 8 \end{pmatrix} \\ (3 \ 4) \otimes \begin{pmatrix} 5 \\ 7 \end{pmatrix} & (3 \ 4) \otimes \begin{pmatrix} 6 \\ 8 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 5 & 10 & 6 & 12 \\ 7 & 14 & 8 & 16 \\ 15 & 20 & 18 & 24 \\ 21 & 28 & 24 & 32 \end{pmatrix}$$

In the following Theorems, we list important properties of the Tracy-Singh product (TS).

Theorem 1.2. [23] Let A, B, C , and D be matrices. Then

- (i) $A \boxtimes B$ and $B \boxtimes A$ exist for any matrices A and B .
- (ii) $A \boxtimes B \neq B \boxtimes A$ in general.
- (iii) $(A \boxtimes B) \boxtimes C = A \boxtimes (B \boxtimes C)$.
- (iv) $(A + B) \boxtimes (C + D) = A \boxtimes C + A \boxtimes D + B \boxtimes C + B \boxtimes D$, if $A + B$ and $C + D$ exist.
- (v) $(A \boxtimes B)(C \boxtimes D) = AC \boxtimes BD$, if AC and BD exist.
- (vi) $(cA) \boxtimes B = c(A \boxtimes B) = A \boxtimes (cB)$.
- (vii) $(A \boxtimes B)^{-1} = A^{-1} \boxtimes B^{-1}$, if A and B are invertible.
- (viii) $(A \boxtimes B)^t = A^t \boxtimes B^t$.
- (ix) $I_n \boxtimes I_m = I_{nm}$ for identity partitioned matrices.

Note that for the Kronecker product of matrices, no partition into blocks is needed.

$$\text{Yet, if } A = \begin{pmatrix} B_{11} & B_{12} & \dots & B_{1s} \\ \dots & \dots & \dots & \dots \\ B_{n1} & B_{n2} & \dots & B_{ns} \end{pmatrix}, \text{ then}$$

$$A \otimes B = \begin{pmatrix} B_{11} \otimes B & B_{12} \otimes B & \dots & B_{1s} \otimes B \\ \dots & \dots & \dots & \dots \\ B_{n1} \otimes B & B_{n2} \otimes B & \dots & B_{ns} \otimes B \end{pmatrix}.$$

In matrix theory, the commutation matrix is used for transforming the vectorized form of a matrix into the vectorized form of its transpose.

Definition 1.3. [18] The *commutation matrix* K_{mn} is the matrix defined by:

$$K_{mn} = \sum_{i=1}^m \sum_{j=1}^n E_{ij} \otimes E_{ij}^t$$

where E_{ij} is a matrix of size $m \times n$ with a 1 in its ij -th position and zeroes elsewhere.

In words, K_{mn} is the square matrix of size mn , partitioned into mn blocks of size $n \times m$ such that the ij -th block has a 1 in its ji -th position and 0 elsewhere, with $K_{nm} = K_{mn}^{-1}$.

For example, $K_{23} = \begin{pmatrix} E_{11} & E_{21} & E_{31} \\ E_{12} & E_{22} & E_{32} \end{pmatrix}$, where E_{ij} are of size 3×2 (see [18, p383]).

Theorem 1.4. [22], [18], [15] Let A be of size $n \times s$ and B of size $m \times t$. Let K_{mn} denote the commutation matrix of size mn as in Definition 1.3. Then

$$(i) \ B \otimes A = K_{mn}(A \otimes B)K_{st}.$$

(ii) If A has a block partition into blocks A_{ij} , $1 \leq i \leq p$, $1 \leq j \leq q$, all of size $n' \times s'$, and B has a block partition into blocks B_{kl} , $1 \leq k \leq u$, $1 \leq l \leq v$, all of size $m' \times t'$:

- $A \boxtimes B = (\mathbf{I}_p \otimes K_{un'} \otimes \mathbf{I}_{m'}) \cdot (A \otimes B) \cdot (\mathbf{I}_q \otimes K_{s't'} \otimes \mathbf{I}_t)$.
- $B \boxtimes A = P \cdot (A \boxtimes B) \cdot Q$.

where P and Q are the following permutation matrices:

$$P = (\mathbf{I}_u \otimes K_{pm'} \otimes \mathbf{I}_{n'}) \cdot K_{mn} \cdot (\mathbf{I}_p \otimes K_{n'u} \otimes \mathbf{I}_{m'})$$

$$Q = (\mathbf{I}_q \otimes K_{vs'} \otimes \mathbf{I}_{t'}) \cdot K_{st} \cdot (\mathbf{I}_v \otimes K_{t'q} \otimes \mathbf{I}_{s'})$$

For more general formulas, in the case that the blocks do not have necessarily the same size, we refer to [15]. From Theorem 1.4 (ii) and (iii), the formulas connecting $A \boxtimes B$ with $B \otimes A$ and with $B \boxtimes A$ are reminiscent to the formula of change of basis, but in general the permutation matrices in Theorem 1.4 (ii) or (iii) are not the inverse one of another.

The TS product of matrices is often called a block Kronecker product, as indeed the result of the product depends on the block partition chosen for each matrix. In the special case of a matrix A of size $n^2 \times p^2$, there exists a unique block partition such that all the blocks are matrices of the same size, that we call *the canonical block partition of A*.

The following matrix is with its canonical partition into

$$\text{blocks, } c = \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ -\frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \end{pmatrix}.$$

It holds that, in the special case that A and B are of size $n^2 \times p^2$ and $m^2 \times q^2$ respectively, with their canonical block partitions, then $A \boxtimes B$ and $A \otimes B$ are similar matrices and the conjugating matrix is a permutation matrix, as described in Proposition 1.5 which is a direct application of Theorem 1.4.

Proposition 1.5. [15, 18, 22] Let A and B of size $n^2 \times p^2$ and $m^2 \times q^2$ respectively, with a canonical block partition (into blocks of the same size $n \times p$ and $m \times q$ respectively). Let K_{mn} denote the commutation matrix of size mn . Then

$$A \boxtimes B = (\mathbf{I}_n \otimes K_{mn} \otimes \mathbf{I}_m) \cdot (A \otimes B) \cdot (\mathbf{I}_p \otimes K_{pq} \otimes \mathbf{I}_q) \quad (1.1)$$

2 APPLICATIONS OF THE TRACY-SINGH IN THE YBE AND CATEGORIES

In the following, given a linear operator $c : V \rightarrow V$, we denote also by c its representing matrix with respect to the standard basis of V , so depending on the context we consider either the operator or the matrix.

2.1 Preliminaries on the Yang-Baxter equation (YBE)

Definition 2.1. [11, Ch.VIII] Let V be a vector space over $\mathbb{C}$. A linear automorphism c of $V \otimes V$ is said to be an R -matrix if it is a solution of the Yang-Baxter equation

$$(c \otimes Id_V)(Id_V \otimes c)(c \otimes Id_V) = (Id_V \otimes c)(c \otimes Id_V)(Id_V \otimes c) \quad (2.1)$$

that holds in the automorphism group of $V \otimes V \otimes V$. It is written as $c^{12}c^{23}c^{12} = c^{23}c^{12}c^{23}$.

Example 2.2. ([13], [11]) Let $c, d : V \otimes V \rightarrow V \otimes V$ be R -matrices, with $\dim(V) = 2$:

$$c = \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ -\frac{1}{\sqrt{2}} & 0 & 0 & \frac{1}{\sqrt{2}} \end{pmatrix} \text{ and } d = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1.5 & 0 \\ 0 & 0 & 0 & 2 \end{pmatrix}$$

Here $c(e_1 \otimes e_2) = \frac{1}{\sqrt{2}} e_1 \otimes e_2 + \frac{1}{\sqrt{2}} e_2 \otimes e_1$, $d(e_1 \otimes e_2) = e_2 \otimes e_1$, with only c unitary. As a convention, we always consider the basis $\{e_i \otimes e_j \mid 1 \leq i, j \leq n\}$ of $V \otimes V$ ordered lexicographically, that is, as an example, for $n = 2$, the ordered basis of $V \otimes V$ is $\{e_1 \otimes e_1, e_1 \otimes e_2, e_2 \otimes e_1, e_2 \otimes e_2\}$.

Any solution c of the YBE yields a family of representations of the braid group B_n :

$$\begin{aligned} \rho_n^c : B_n &\rightarrow \text{GL}((\mathbb{C}^d)^{\otimes n}) \\ \sigma_j &\mapsto (Id_d)^{\otimes j-1} \otimes c \otimes (Id_d)^{\otimes n-j-1} \\ &\text{where } c : (\mathbb{C}^d)^{\otimes 2} \rightarrow (\mathbb{C}^d)^{\otimes 2} \text{ and} \\ &\sigma_1, \sigma_2, \dots, \sigma_{n-1} \text{ are generators of } B_n. \end{aligned} \quad (2.2)$$

We recall two facts important for the computations: ρ_n^c is a homomorphism of groups and the property $(A \otimes B)(C \otimes D) = AC \otimes BD$ holds only if AC and BD exist. As an example, if $b = \sigma_3 \sigma_4 \sigma_3 \in B_n$, where $n = 5$, then we have the following computation:

$$\begin{aligned} \rho_n^c(b) &= ((Id_d)^{\otimes 2} \otimes c \otimes (Id_d)^{\otimes 1}) \cdot \\ &\quad ((Id_d)^{\otimes 3} \otimes c \otimes (Id_d)^{\otimes 0}) \cdot \\ &\quad ((Id_d)^{\otimes 2} \otimes c \otimes (Id_d)^{\otimes 1}) \\ &= (Id_d)^{\otimes 2} \otimes ((c \otimes Id_d)(Id_d \otimes c)(c \otimes Id_d)) \end{aligned} \quad (2.3)$$

As c satisfies Eq. (2.1), we have indeed that $\rho_n^c(\sigma_3 \sigma_4 \sigma_3) = \rho_n^c(\sigma_4 \sigma_3 \sigma_4)$.

Definition 2.3. [24] Let $c : (\mathbb{C}^d)^{\otimes 2} \rightarrow (\mathbb{C}^d)^{\otimes 2}$ be a solution of the YBE. Let $\mu \in \text{End}(\mathbb{C}^d)$. Let ρ_n^c be defined as in Eq. (2.2). A pair (c, μ) is an *enhanced YBE pair* if

- (i) c commutes with $\mu \otimes \mu$
- (ii) $\text{Tr}_2(c \circ \mu^{\otimes 2}) = \text{Tr}_2(c^{-1} \circ \mu^{\otimes 2}) = \mu$, where Tr_2 denotes the partial trace over the second factor.

Any oriented link is equivalent (ambient isotopic) to the trace closure of some braid b , as illustrated in Figure 2.1. Using that fact, V. Turaev shows in [24], that if

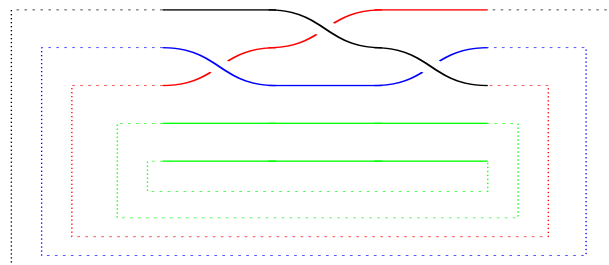


Figure 2.1: The trace closure of the braid $\sigma_3 \sigma_4 \sigma_3$ in B_5 (c, μ) is an enhanced YBE pair, then there is an appropriately normalized trace $(I_c(b), b \in B_n)$ of the representations ρ_n^c , that yields a link invariant:

$$I_c(b) = \text{Tr}(\rho_n^c(b) \circ \mu^{\otimes n}) \quad (2.4)$$

As an example, if (c, μ) is an enhanced YBE pair, $b = \sigma_3 \sigma_4 \sigma_3 \in B_5$, then from (2.3)-(2.4):

$$\begin{aligned} I_c(b) &= \text{Tr}(\rho_n^c(b) \circ \mu^{\otimes 10}) = \\ &= \text{Tr}(((Id_d)^{\otimes 2} \otimes (c \otimes Id_d)(Id_d \otimes c)(c \otimes Id_d))) \mu^{\otimes 5}) \\ &= \text{Tr}(\mu^{\otimes 2} \otimes ((c \otimes Id_d)(Id_d \otimes c)(c \otimes Id_d) \mu^{\otimes 3})) \\ &= \text{Tr}(\mu)^2 \text{Tr}((c \otimes Id_d)(Id_d \otimes c)(c \otimes Id_d) \mu^{\otimes 3}) \end{aligned} \quad (2.5)$$

The link invariant defined by Turaev is a generalisation of the Jones link invariant. Indeed, for the following specific matrices c and μ with coefficients in $\mathbb{Z}[\sqrt{t}, \frac{1}{\sqrt{t}}]$ instead of $\mathbb{C}$:

$$c = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & -\sqrt{t} & 0 \\ 0 & -\sqrt{t} & 1-t & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \mu = \begin{pmatrix} 1 & 0 \\ 0 & t \end{pmatrix}$$

$I_c(b)$ is equal to the Jones polynomial, up to some normalisation.

2.2 Applications of the Tracy-Singh product for solutions of the YBE

In [3, 4], it is shown that the TS product of linear operators (or matrices), with the canonical block partition, is an efficient tool to construct linear operators (or matrices) that preserves many of their properties. More precisely:

Theorem 2.4. [3, 4] Let $c, c' : (\mathbb{C}^d)^{\otimes 2} \rightarrow (\mathbb{C}^d)^{\otimes 2}$ be linear operators. Let $\mu, \eta \in \text{End}(\mathbb{C}^d)$. Let $c \boxtimes c' : (\mathbb{C}^{d^2})^{\otimes 2} \rightarrow (\mathbb{C}^{d^2})^{\otimes 2}$ be the linear operator obtained from $c \boxtimes c'$, the TS product of c and c' with the canonical block partition for both matrices.

- (i) If c and c' are automorphisms, then $c \boxtimes c'$ is also an automorphism.
- (ii) If c and c' are unitary, then $c \boxtimes c'$ is also unitary.
- (iii) If c and c' are R -matrices, then $c \boxtimes c'$ is also a R -matrix.
- (iv) If (c, μ) and (c', η) are enhanced YBE pairs, then $(c \boxtimes c', \mu \otimes \eta)$ is also an enhanced YBE pair.

It results from Theorem 2.4, that the TS product, with the canonical block partition, enables the construction of infinite families of solutions of the YBE. A question that arises naturally, is why looking at the Tracy-Singh product of R -matrices c and c' and not at their Kronecker product $c \otimes c'$. The reason is that $c \otimes c'$ is not necessarily a R -matrix. Indeed, a simple computation shows that for c from Example 2.2, $c \otimes c$ does not satisfy the YBE.

In the case that c and c' are R -matrices, their TS product with the canonical block partition coincides with

the operation called *the tensor product of R-matrices* in [5, 16], although it differs from the actual tensor product $\otimes$. Indeed, in that specific case, Proposition 1.5 implies that the TS product represents the linear transformation $F_{23}(c \otimes c')F_{23} : \mathbb{C}^d \otimes \mathbb{C}^d \otimes \mathbb{C}^d \otimes \mathbb{C}^d \rightarrow \mathbb{C}^d \otimes \mathbb{C}^d \otimes \mathbb{C}^d \otimes \mathbb{C}^d$, where F_{23} exchanges the two middle factors [3]. More generally, if A and B are of size $n^2 \times p^2$ and $m^2 \times q^2$ respectively, with a canonical partition, then it results from Equation (1.1) that their Tracy-Singh product represents a linear transformation $c \boxtimes d : \mathbb{C}^n \otimes \mathbb{C}^m \otimes \mathbb{C}^n \otimes \mathbb{C}^m \rightarrow \mathbb{C}^p \otimes \mathbb{C}^q \otimes \mathbb{C}^p \otimes \mathbb{C}^q$ of the form $F_{23}(c \otimes d)F_{23}$, where $c : (\mathbb{C}^n)^{\otimes 2} \rightarrow (\mathbb{C}^p)^{\otimes 2}$ and $d : (\mathbb{C}^m)^{\otimes 2} \rightarrow (\mathbb{C}^q)^{\otimes 2}$, and F_{23} exchanges the two middle factors.

The cabling operation of R -matrices is defined in [25] to construct new solutions of the YBE from an existing one. It is induced from the cabling of braids, which consists roughly in multiplying the strings in a given braid. S. Majid suggested there may be some connection between the cabling operation and the TS product of solutions of the YBE ([19] and see [20] for reference). This is a direction of current research we are interested in. Indeed, we study whether there is a connection between the cabling operation and the TS product of solutions of the YBE and if the answer is positive to understand its nature. Furthermore, we explore the possible implications of these constructions in the context of quantum computation and the design of quantum circuits.

2.3 Applications of the Tracy-Singh product in monoidal categories

The Tracy-Singh product of matrices has also a surprising connection with a categorical construction that we describe in the following. Indeed, it can be defined as the monoidal product (or a tensor functor) in a particular category of vector spaces, in which the canonical partition into blocks is ensured.

The category Vec is a symmetric monoidal category, with objects all the finite dimensional vector spaces over a fixed field, let's say $\mathbb{C}$, and morphisms the linear transformations between vector spaces. The monoidal product is the functor $\otimes : \text{Vec} \times \text{Vec} \rightarrow \text{Vec}$ that sends each pair of objects (U, V) to $U \otimes V$ and each pair of morphisms (f, g) to $f \otimes g$, and its unit object is $\mathbb{C}$. Furthermore, $\text{Vec} \otimes \text{Vec}$ can be defined and it is also a symmetric category [8, Section 4.6], [7, Lecture 9, p.90], with the following particular symmetric subcategory:

$$\text{Diag} = \{U \otimes U \mid U \in \text{Vec}\} \subset \text{Vec} \otimes \text{Vec}$$

In [3], it is proved that the Tracy-Singh product of the representing matrices (with respect to standard bases for example) of morphisms c and c' in the category Diag is a functor, and it can be defined as the monoidal product in $\text{Mor}(\text{Diag})$. As we recall, to apply the

Tracy-Singh product on matrices they have to be partitioned into blocks. If the matrices have arbitrary sizes, they cannot be necessarily partitioned into blocks of the same size. However, if a matrix A has size of the form $n^2 \times p^2$, n, p not necessarily different, then there is a canonical partition of A , where all the blocks have the same size $n \times p$. The existence of such a canonical partition is ensured for representing matrices of morphisms in Diag , but not in $\text{Vec} \otimes \text{Vec}$ in general.

3 APPLICATIONS OF THE TRACY-SINGH PRODUCT IN QUANTUM COMPUTING

3.1 Preliminaries on quantum computing and quantum entanglement

We follow the presentation from the reference books on the topic [21], [9] and the papers [2], [12, 13, 14] and we refer to these references and the vast literature for more details.

Definition 3.1. Let $\mathbb{C}^2$ be the two-dimensional Hilbert space with two orthonormal state vectors, denoted by $|0\rangle$ and $|1\rangle$, that form a basis in bijection with the standard basis $\{(1, 0), (0, 1)\}$. A *qubit (or quantum bit)* is a state vector in $\mathbb{C}^2$

$$|\phi\rangle = \alpha |0\rangle + \beta |1\rangle \quad (3.1)$$

where $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$. We say that any linear combination of the form (3.1) is a *superposition of the states $|0\rangle$ and $|1\rangle$* , with *amplitude α* for the state $|0\rangle$ and *β* for the state $|1\rangle$.

Intuitively, the states $|0\rangle$ and $|1\rangle$ are analogous to the two values 0 and 1 which a bit may take. The way a qubit differs from a bit is that superposition of these two states, of the form (3.1), can also exist, in which it is not possible to say that the qubit is definitely in the state $|0\rangle$ or definitely in the state $|1\rangle$. A measurement of a qubit $|\phi\rangle = \alpha |0\rangle + \beta |1\rangle$ provides as output the bit 0 with probability $|\alpha|^2$ and the bit 1 with probability $|\beta|^2$ and the state $|\phi\rangle$ collapses to $|0\rangle$ or $|1\rangle$. After the measurement, all the information about the superposition is irreversibly lost. Examples of qubits include the spin of the electron in which the two basis states are spin up and spin down, and in this case the basis is denoted by $\{|\uparrow\rangle, |\downarrow\rangle\}$; or the polarization of a single photon in which the two basis states are vertical and horizontal, and in this case the basis is denoted by $\{|\rightarrow\rangle, |\leftarrow\rangle\}$.

More generally, a *n-qubit* is a state vector in the 2^n -dimensional Hilbert space, with an orthonormal basis $\{|\psi_i\rangle \mid 1 \leq i \leq 2^n\}$ in bijection with the standard basis, of the form

$$|\phi\rangle = \sum_{i=1}^{i=2^n} \alpha_i |\psi_i\rangle \quad (3.2)$$

where $\alpha_i \in \mathbb{C}$, $1 \leq i \leq 2^n$, and $\sum_{i=1}^{i=2^n} |\alpha_i|^2 = 1$. As an example, a two-qubit has the form

$$|\phi\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle \quad (3.3)$$

In analogy with the case of a qubit, a measurement of a n -qubit of the form (3.2) gives as outcome n bits, each n -tuple of bits with a precalculated probability. Moreover, the state $|\phi\rangle$, in the superposition of the 2^n basis states, collapses to just one of the basis states.

Definition 3.2. Let $\mathbb{C}^d$ be the d -dimensional Hilbert space with orthonormal base denoted by $|0\rangle, |1\rangle, \dots$, and $|d-1\rangle$. A *qudit* is a state vector in $\mathbb{C}^d$, where $\alpha_i \in \mathbb{C}$ and $\sum_{i=1}^{i=d} |\alpha_i|^2 = 1$:

$$|\phi\rangle = \alpha_1 |0\rangle + \dots + \alpha_d |d-1\rangle \quad (3.4)$$

Any linear combination of the form (3.4) is a *superposition of the states* $|0\rangle, \dots, |d-1\rangle$.

A qubit is a special case of a qudit, for the case $d = 2$. A *n-qudit* is a state vector in the Hilbert space $(\mathbb{C}^d)^{\otimes n}$. A quantum system with one state vector $|\phi\rangle$ is called a *pure state*. However, it is also possible for a system to have a set of potential different state vectors. As an example, there may be a probability $\frac{1}{2}$ that the state vector is $|\phi\rangle$ and a probability $\frac{1}{2}$ that the state vector is $|\psi\rangle$. This system is said to be in a *mixed state*. There exists a matrix called density matrix which trace value determines whether a system is in a pure or a mixed state [21, p.99].

Definition 3.3. A n -qudit $|\phi\rangle$ is *decomposable* if $|\phi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle \otimes \dots \otimes |\phi_n\rangle$, where $|\phi_i\rangle \in \mathbb{C}^d$, for $1 \leq i \leq n$. Otherwise, $|\phi\rangle$ is *entangled*.

As an example, $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is an entangled two-qubit, since it cannot be decomposed as a tensor product of two qubits. In general, a two-qubit pure state $|\phi\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle$ is entangled if and only if $\alpha_{00}\alpha_{11} - \alpha_{01}\alpha_{10} \neq 0$. In [?], the authors give a combinatorial criteria to determine whether a n -qubit is entangled or not.

Any quantum evolution of a n -qudit, or any quantum operation on a n -qudit is described by a unitary operator or square unitary matrix of size d^n , called a (*quantum*) *n-qudit gate*, which transforms $|\phi\rangle = \sum_{i=1}^{i=d^n} \alpha_i |\psi_i\rangle$ into another linear combination of the (standard) basis states $\{|\psi_i\rangle \mid 1 \leq i \leq d^n\}$.

Example 3.4. Let c be the unitary R -matrix from Example 2.2. So, c is a 2-qubit (YBE) gate and it acts on the basis states $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ of $(\mathbb{C}^2)^{\otimes 2}$, with $|00\rangle = |0\rangle \otimes |0\rangle$, $|01\rangle = |0\rangle \otimes |1\rangle$, and so on,

such that $c |00\rangle = \frac{1}{\sqrt{2}} |00\rangle - \frac{1}{\sqrt{2}} |11\rangle$, $c |01\rangle = \frac{1}{\sqrt{2}} |01\rangle + \frac{1}{\sqrt{2}} |10\rangle$, $c |10\rangle = -\frac{1}{\sqrt{2}} |01\rangle + \frac{1}{\sqrt{2}} |10\rangle$ and $c |11\rangle = \frac{1}{\sqrt{2}} |00\rangle + \frac{1}{\sqrt{2}} |11\rangle$.

Example 3.5. A very important example of 2-qubit gate is the following unitary square matrix of size 4 which

acts on 2-qubits: $CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$; not an R -matrix.

Definition 3.6. [2] A 2-qudit gate $L: (\mathbb{C}^d)^{\otimes 2} \rightarrow (\mathbb{C}^d)^{\otimes 2}$ is *primitive* if L maps decomposable 2-qudit to decomposable 2-qudit, otherwise L is said to be *imprimitive*.

In other words, a 2-qudit gate L is said to be *imprimitive*, if there exists a decomposable 2-qudit $|\phi\rangle$ such that $L|\phi\rangle$ is an entangled 2-qudit. An imprimitive 2-qudit gate is often called *entangling*, as in [13]. There is a criteria to determine whether a 2-qudit is primitive.

Theorem 3.7. [2] Let $P: (\mathbb{C}^d)^{\otimes 2} \rightarrow (\mathbb{C}^d)^{\otimes 2}$ denote the swap gate, that is the 2-qudit gate such that $P|\alpha\beta\rangle = |\beta\alpha\rangle$. Let $L: (\mathbb{C}^d)^{\otimes 2} \rightarrow (\mathbb{C}^d)^{\otimes 2}$ be a 2-qudit gate. Then L is primitive if and only if $L = L_1 \otimes L_2$ or $L = (L_1 \otimes L_2)P$, for some 1-qudit gates L_1, L_2 .

In [13], the authors answer the question of which 2-qubit gates which satisfy the YBE are entangling, using the classification from [6] and the criteria for entanglement from [2]. The 2-qubit gates from Examples 3.4 and 3.5 are both entangling operators [9, 13, 21]. Note that not every 2-qubit gate that is an R -matrix is en-

tangling. Indeed, let $c_{2,1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ be a R -

matrix of size 4. It is easy to show that the 2-qubit gate $c_{2,1}$ is primitive. Let $|\phi\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle$ be a decomposable two-qubit pure state, that is $\alpha_{00}\alpha_{11} - \alpha_{01}\alpha_{10} = 0$. Then $c_{2,1}|\phi\rangle = \alpha_{00} |00\rangle + \alpha_{10} |01\rangle + \alpha_{01} |10\rangle + \alpha_{11} |11\rangle$ and $\alpha_{00}\alpha_{11} - \alpha_{10}\alpha_{01} = 0$, that is $c_{2,1}|\phi\rangle$ is decomposable.

3.2 Applications of the Tracy-Singh product in quantum computing

The Tracy-Singh product is an efficient tool to create entangling and primitive 2-qudit gates, as it preserves these properties in the following way:

Theorem 3.8. [3] Let $c: (\mathbb{C}^n)^{\otimes 2} \rightarrow (\mathbb{C}^n)^{\otimes 2}$ and $c': (\mathbb{C}^m)^{\otimes 2} \rightarrow (\mathbb{C}^m)^{\otimes 2}$ be 2-qudit gates. Let $c \boxtimes c'$ denote their Tracy-Singh product, with the canonical block partition.

(i) Assume c is entangling. Then $c \boxtimes c' : (\mathbb{C}^{nm})^{\otimes 2} \rightarrow (\mathbb{C}^{nm})^{\otimes 2}$ is also entangling.

(ii) Assume c and c' are primitive. If $c = c_1 \otimes c_2$ and $c' = c'_1 \otimes c'_2$ or $c = (c_1 \otimes c_2)S_c$ and $c' = (c'_1 \otimes c'_2)S_{c'}$, where S_n and S_m are the swap maps on $(\mathbb{C}^n)^{\otimes 2}$ and $(\mathbb{C}^m)^{\otimes 2}$ respectively. Then $c \boxtimes c' : (\mathbb{C}^{nm})^{\otimes 2} \rightarrow (\mathbb{C}^{nm})^{\otimes 2}$ is also primitive (of the same kind).

Combining Theorem 2.4 with Theorem 3.8 ensures the existence of entangling and primitive 2-qudit YBE gates for every $d \geq 2$. More precisely:

Theorem 3.9. [3] Let $d \geq 2$ be any integer. Then, there exists an entangling 2-qudit YBE gate $U : (\mathbb{C}^d)^{\otimes 2} \rightarrow (\mathbb{C}^d)^{\otimes 2}$ and a primitive 2-qudit YBE gate $S : (\mathbb{C}^d)^{\otimes 2} \rightarrow (\mathbb{C}^d)^{\otimes 2}$.

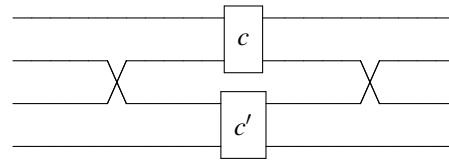
Note that, in the same way that an entangling 2-qudit (YBE or not) gate is not the tensor product of two gates, an arbitrary 2-qudit (YBE or not) gate is not necessarily the TS product of two gates. If the theory develops, maybe a name should be coined to describe that.

Definition 3.10. [2] A collection $\mathcal{U}$ of 1-qudit gates $\{S_i\}$ and 2-qudit gates $\{U_j\}$ is called *universal* if, for each $n \geq 2$, every n -qudit gate can be approximated with arbitrary accuracy by a circuit made up of the n -qudit gates produced by the $\{S_i\}$ and $\{U_j\}$, and it is called *exactly universal* if, for each $n \geq 2$, every n -qudit gate can be obtained exactly by a circuit made up of the n -qudit gates produced by the $\{S_i\}$ and $\{U_j\}$.

In [2], it is proved that U is entangling if and only if U is exactly universal, which means that the collection of all 1-qudit gates together with U generates the unitary group $U((\mathbb{C}^d)^{\otimes n})$, for every $n \geq 2$. Since for every integer $d \geq 2$, there exists an entangling 2-qudit gate $U : (\mathbb{C}^d)^{\otimes 2} \rightarrow (\mathbb{C}^d)^{\otimes 2}$, where U satisfies the YBE (Theorem 3.9), one can assume that for every $d \geq 2$, there exists an exactly universal set of gates $\mathcal{U}_d$ with a single 2-qudit gate U . This enables to show that, whenever the realisation of the gates $c, c' : (\mathbb{C}^d)^{\otimes 2} \rightarrow (\mathbb{C}^d)^{\otimes 2}$ in terms of gates from $\mathcal{U}_d$ is given, there is a simple way to realise the 4-qudit gate $c \boxtimes c' : (\mathbb{C}^d)^{\otimes 4} \rightarrow (\mathbb{C}^d)^{\otimes 4}$ in terms of the gates from $\mathcal{U}_d$ [4]. That is, although the TS product of matrices is quite esoteric, its implementation is in fact simple. Indeed:

Proposition 3.11. [4] Let $c, c', P : (\mathbb{C}^d)^{\otimes 2} \rightarrow (\mathbb{C}^d)^{\otimes 2}$ be 2-qudit gates, with P the swap map. Let $c \boxtimes c' : (\mathbb{C}^d)^{\otimes 4} \rightarrow (\mathbb{C}^d)^{\otimes 4}$ be the 4-qudit gate defined by their Tracy-Singh product $c \boxtimes c'$ with the canonical block

partition. Then $c \boxtimes c' = (\mathbf{I}_d \otimes P \otimes \mathbf{I}_d)(c \otimes c')(\mathbf{I}_d \otimes P \otimes \mathbf{I}_d)$:



From Theorems 3.8-3.9, given an entangling 2-qudit gate it is possible to create infinitely many other entangling gates with the TS product, and each of them can be included in an exactly universal set of gates $\mathcal{U}_d$. A question that arises naturally is which gate is it "better" to insert in $\mathcal{U}_d$, the original one or one of the gates obtained in the process. Another natural question is whether universal gates obtained from the TS product offer more advantages in terms of implementation than other universal gates.

The question whether a YBE gate is primitive has found an interesting application in the domain of knot invariants. Indeed, in [1], the authors prove that if a YBE gate c is primitive, then the link invariant I_c obtained from c , using the Turaev construction, is trivial, and that the converse is not necessarily true. Indeed, they give an example of entangling YBE gate that leads to a trivial link invariant. Furthermore, if (c, μ) and (c', η) are enhanced YBE pairs, such that c and c' are primitive of the same kind, and μ, η are invertible, then $I_{c \boxtimes c'}(b) = I_c(b) \cdot I_{c'}(b)$, for every $b \in B_n$ [4]. It would be interesting to understand whether the connection between primitive gates and link invariants is purely theoretical, or it could be useful to identify quantum advantages.

To conclude this paper, we would like to point on some more open questions and future directions of research which are in direct continuation with the results in this paper. It would be interesting to explore if there are some specific algorithms for which the use of gates obtained from the TS product offers some advantages in circuit depth or on other parameters to be defined and leads to a more efficient implementation. It would be also interesting to study the robustness of the TS generated gates to common noise model and explore implementations for specific hardware platforms. The creation of an open-source software library that implements the TS generated gates and its use in gate synthesis for popular quantum computing frameworks may be useful to increase the list of gates.

A question of particular interest in a more mathematical viewpoint is the following: how does the fact that c is an entangling or a primitive gate influence the link invariant I_c ? Every YBE 2-qudit gate (or R -matrix) c induces a representation ρ_n^c of the braid group B_n as defined in Equation (2.2) and a link invariant I_c as defined in Equation (2.4). In [1], the authors answer partially the question cited above. Indeed, they show that if c

is a primitive YBE gate, then I_c is trivial and that the converse is not always true. It would be interesting to understand whether there exist some other connections between the properties of the YBE gate and link invariants in general.

Acknowledgment. I would like to thank the anonymous reviewers for their helpful comments and feedback, and their many insightful comments and suggestions which greatly strengthened the overall manuscript and opened horizons of future research.

4 REFERENCES

- [1] G. Alagic, M. Jarret, S.P. Jordan, *Yang-Baxter operators need quantum entanglement to distinguish knots*, J. of Physics A: Mathematical and Theoretical, **49**(2016), n.7.
- [2] J.L. Brylinski, R. Brylinski, *Universal quantum gates*, Mathematics of Quantum Computation, Chapman and Hall/CRC Press, Boca Raton, Florida 2002 (edited by R. Brylinski and G. Chen).
- [3] F. Chouraqui, *The Yang-Baxter equation, quantum computing and quantum entanglement*, Physica Scripta **99** (2024), n. 11.
- [4] F. Chouraqui, *On the Realization of quantum gates coming from the Tracy-Singh product*, Quantum Inf. Process **24** (2025), 261.
- [5] R. Conti, G. Lechner, *Yang-Baxter endomorphisms*, J. London Math. Soc. (2) **103** (2021), 633-671.
- [6] H. Dye, *Unitary solutions to the Yang-Baxter equation in dimension four*, Quantum Information Processing, Vol. 2, nos. 1-2, April 2003, 117-150.
- [7] P. Etingof, *Topics in Lie Theory: Tensor Categories, course 18.769, Spring 2009*, MIT OpenCourseWare, <https://ocw.mit.edu/courses/18-769-topics-in-lie-theory-tensor-categories-spring-2009/pages/lecture-notes>.
- [8] P. Etingof, S. Gelaki, D. Nikshych, V. Ostrik, *Tensor categories*, Mathematical surveys and monographs **205**, American Mathematical Society.
- [9] J. Gruska, *Quantum Computing*, McGraw-Hill Companies, London 1999.
- [10] D.C. Hyland, E.G. Collins, Jr., *Block Kronecker Products and Block Norm Matrices in Large-Scale Systems Analysis*, SIAM J. Matrix Anal. Appl. **10** (1989), 18-29.
- [11] C. Kassel, *Quantum groups*, Graduate Texts in Mathematics **155** (1995), Springer Verlag, Berlin.
- [12] L.H. Kauffman, S.J. Lomonaco Jr., *Quantum entanglement and topological entanglement*, New J. Phys. **4**, 73, 2002.
- [13] L.H. Kauffman, S.J. Lomonaco Jr., *Braiding Operators are Universal Quantum Gates*, New J. Phys. **6** (2004).
- [14] L.H. Kauffman, E. Mehrotra, *Topological aspects of quantum entanglement*, Quantum Inf. Process **18**, 76 (2019).
- [15] R.H. Koning, H. Neudecker, T. Wansbeek, *Block Kronecker products and the vecb operator*, Linear Algebra and its applications **149** (1991), 165-184.
- [16] G. Lechner, U. Pennig, S. Wood, *Yang-Baxter representations of the infinite symmetric group*, Adv. Math **355** (2019), 1-42.
- [17] S. Liu, *Matrix results on the Khatri-Rao and Tracy-Singh products*, Linear Algebra and its Applications **289** (1999), 267-277.
- [18] J.R. Magnus, H. Neudecker, *The commutation matrix: some properties and applications*, Annals of Statistics **7**(1979), 381-394.
- [19] S. Majid, *Personal communication*, 2024.
- [20] S. Majid, *Foundations of Quantum Group Theory*, Cambridge University Press, 1995.
- [21] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press 2000.
- Extraspecial two-Groups, generalized Yang-Baxter equations and braiding quantum gates*, Quant. Inf. Comput. **10** (2010), 685-702.
- [22] D. S. Tracy, K. G. Jinadasa, *Partitioned Kronecker products of matrices and applications*, Canad. J. Statist. **17** (1989), 107-120.
- [23] D.S. Tracy, R.P. Singh, *A new matrix product and its applications in partitioned matrix differentiation*, Statistica Neerlandica **26** (1972), 143-157.
- [24] V. Turaev, *The Yang-Baxter equation and invariants of links*, Invent. Math, **92** (1988), 527-553.
- [25] H. Wenzl, *Representations of braid groups and the quantum Yang-Baxter equation*, Pacific J. Math. **145** (1990), n.1, 153-180.

