Josai Mathematical Monographs
Vol. 11 (2018) pp. 87–96

Quantum gates and TQC

Jun Ichi Fujii

Abstract. The TQC theory based on non-abelian anyons is one of remarkable approaches to realize quantum computer. Surveying this theory, we observe how to construct quantum gates by a Fibonacci anyon, a typical non-abelian one.

1. Introduction

There are many approaches to realize quantum computers as in the following figure:

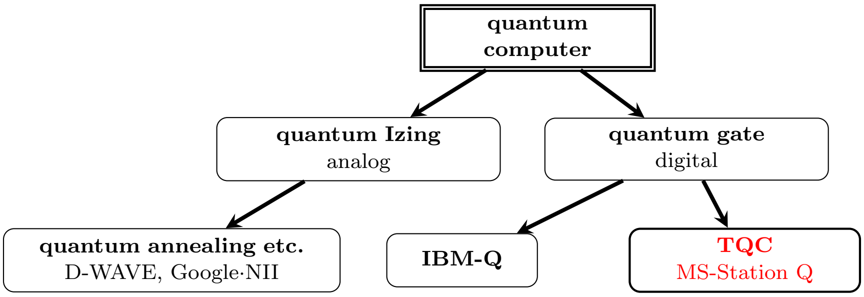


Figure 1.

Among others, we are interested in the **topological quantum computing (TQC)** method supported by Microsoft, which is related to many mathematical and physical fields; knot theory, braid theory, quantum groups, conformal field theory(WZW model or Chern-Simons theory), string theory and so on. In this method, the main concept is **non-abelian anyon**, which is quasi-particle related to quantum Hall effects or quantum vortex. These particles are paraphrased in the following way:

- Boson: $|y\rangle \otimes |x\rangle \sim |x\rangle \otimes |y\rangle$ • Fermion: $|y\rangle \otimes |x\rangle \sim -|x\rangle \otimes |y\rangle$
- (abelian) anyon: $|y\rangle \otimes |x\rangle \sim e^{it}|x\rangle \otimes |y\rangle$
- (non-abelian) anyon: $|y\rangle \otimes |x\rangle \sim e^{iH}(|x\rangle \otimes |y\rangle)$

2010 Mathematics Subject Classification. Primary 81P45; Secondary 81T45, 81U20 .
Key Words and Phrases. Topological quantum computing, quantum gates, Fibonacci anyon.

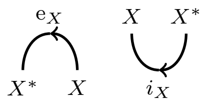
Making use of this non-abelian property, topological quantum computing is done by braiding strings as world lines of (quasi)particles as in the picture on the front page in [3].

In this paper, surveying TQC, we observe how quantum gates are constructed in the above way.

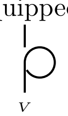
2. Modular category as a model of TQC

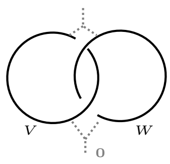
TQC theory is based on various mathematical theories. Here we give one of models; **modular tensor category (MTC)**, see [15, 17] for direct relation between TQC and MTC, see also [1, 4, 5, 10](see [11] for categorical basics).

A MTC $\mathcal{C} = (\mathcal{C}, \mathcal{V})$ is a semisimple Ribbon category with the nondegenerate **modular S-matrix** S:

- The direct sum $\oplus$ as the biproduct and the **dual** X^* of a object X are defined:
  The dual is determined by morphisms e_X and i_X 

- The objects are generated by the simple objects $\{V_j | j \in J\}$;
  $$X = \oplus_{j \in J} N_j V_j \quad \big(N_j = \dim \mathbf{Hom}(X, V_j)\big).$$
  The set $\mathcal{V} = \{V_j\}$ is finite and self-dual: $V_j^* \in \{V_j\}$.
  The **vacuum** V_0 exists in $\mathcal{V}$; $V_0 \otimes A = A \otimes V_0 = A$.
- The following isomorphisms are equipped:
  braiding $\sigma_{V,W}$ 

  , **twist** θ_V 

  $\theta_{V \otimes W} = \theta_V \otimes \theta_W \, \sigma_{W,V} \sigma_{V,W}$
- Morphisms $\mathbf{Hom}(A, B)$ are finite dimensional $\mathbb{C}$ vector space. In particular, $\mathbf{Hom}(V_i, V_j) = \{0\}$ if $i \neq j$ and $\mathbf{End}(V_j) = \mathbf{Hom}(V_j, V_j) = \mathbb{C}$.
- **modularity**: $S = (s_{ij})$ is invertible; $s_{ij} =$ 

By the above definition, for $X = \oplus_j N_j V_j$, we have

$$\mathbf{Hom}(X, V_k) = \bigoplus_j \mathbf{Hom}(V_j, V_k)^{N_j} = \mathbf{Hom}(V_k, V_k)^{N_k} = \mathbb{C}^{N_k},$$

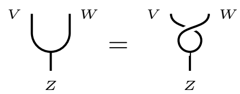
and also $\mathbf{Hom}(V_k, X) = \mathbb{C}^{N_k}$. In particular, for simple objects,

$$N_{ij}^k \equiv \dim \mathbf{Hom}(V_i \otimes V_j, V_k) = \dim \mathbf{Hom}(V_k, V_i \otimes V_j).$$

This guarantees the **fusion** (or **splitting**) property:

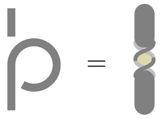
$$V_i \otimes V_j = \bigoplus_k N_{ij}^k V_k$$

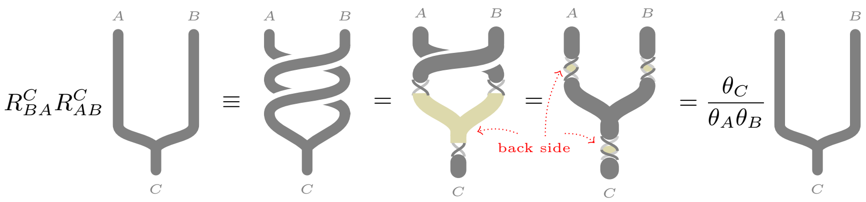
and N_{ij}^k is called the **fusion coefficient**. Thus MTC is equipped with braidings and fusion structure. The anyons in TQC is considered as a simple object V_j or its morphism id_{V_j} as a string (or its representation) in MTC.

The term 'Ribbon' comes from the following fact: We can use the framed string (called ribbon) instead of string in TQC to see braidings and twists. For example, we show the following formula for the **rotation** R_{VW}^Z: 

.

THEOREM 2.1 (**monodromy equation**). $R_{WV}^Z R_{VW}^Z = \dfrac{\theta_Z}{\theta_V \theta_W} I.$

PROOF. By θ_V =  , transforming $V, W, Z \mapsto A, B, C$ as framed strings, we have



,

which shows the monodromy equation. □

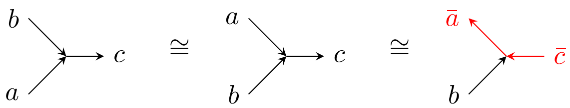
3. Fusion in TQC

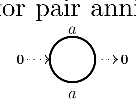
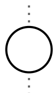
In this section, the references are [7, 4, 2, 12, 14, 16, 18]. Afterwards, let $\mathcal{F}$ be the finite self-dual set of particles, $\mathbf{0}$ the vacuum one ($N_{a\mathbf{0}}^x = N_{\mathbf{0}a}^x = \delta_{a,x}$.), $\bar{a}$ the dual of $a \in \mathcal{F}$ which is considered as the **anti-particle** of a.

Then the fusion structure is expressed as (where $\oplus_{\mu=1}^{0} x = 0$ for convenience)

$$a \otimes b \to \bigoplus_{x\in\mathcal{F}} N_{ab}^{x} x = \sum_{x\in\mathcal{F}} N_{ab}^{x} x = \sum_{x\in\mathcal{F}} \bigoplus_{\mu=1}^{N_{ab}^{x}} x \qquad N_{ab}^{x} \in \mathbb{N} \cup \{0\}\,. \tag{1}$$

Moreover the fusion coefficients satisfy $N_{ba}^{c} = N_{ab}^{c} = N_{b\bar{c}}^{\bar{a}}$ by the following identification since $\bar{a}$ can be expressed as the reversed arrow for a:

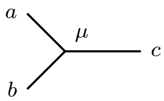


For the pair of a and its dual $\bar{a}$, the fusion for pair annihilation is $a \otimes \bar{a} \to \mathbf{0}$ and the splitting for pair creation is $\mathbf{0} \to a \otimes \bar{a}$;  , which defines the scalar **quantum trace** $d_a \equiv \mathrm{Tr}\, a =$  . Taking trace for $a \otimes b = \sum_x N_{a,b}^{x} x$, we have

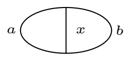
THEOREM 3.1. $$d_a d_b = \sum_x N_{a,b}^{x} d_x = \sum_x (\mathbf{N}_a)_{bx} d_x.$$

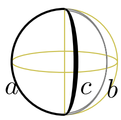
As a consequence, we can take d_a as a positive number by virtue of Perron-Frobenius theorem for nonnegative matrix $\mathbf{N}_a$.

Note that the above fusion tree has the multiplicity as in (1), so we must express it in an exact discussion:

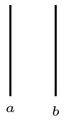
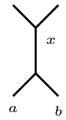
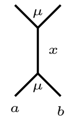


$$\mu = 1, 2, ..., N_{ab}^{c}.$$

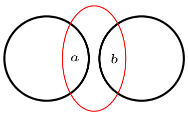
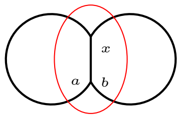
To see some important formulas, we introduce θ-net $\Theta(a, b, x) =$  (It is 0 if it cannot be defined); $N_{a,b}^{x} = 0 \iff \Theta(a, b, x) = 0$. For convenience, we define $N_{a,b}^{x}/\Theta(a, b, x) = 0$ in this case. Moreover, observing θ-net in 3 dimensions as 3 half-circles, we may consider

$$\Theta(a, b, c) =$$  $$= \sqrt{d_a d_b d_c}.$$

Then we have the following fusion formula

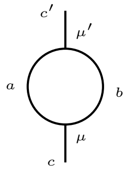
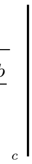
THEOREM 3.2.  $= \sum_x \frac{N_{a,b}^x d_x}{\Theta(a,b,x)}$  $= \sum_{x,\mu} \sqrt{\frac{d_x}{d_a d_b}}$  .

PROOF. Observing the following circled parts in red at both ends;

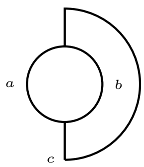
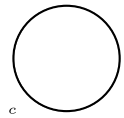
 $= d_a d_b = \sum_x N_{a,b}^x d_x = \sum_x \frac{N_{a,b}^x d_x}{\Theta(a,b,x)}$  ,

we have the required formula. □

Next we also the bubble-removing formula:

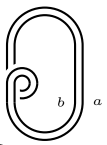
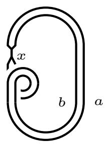
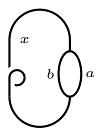
THEOREM 3.3.  $= \delta_{c,c'} \delta_{\mu,\mu'} \sqrt{\frac{d_a d_b}{d_c}}$ 

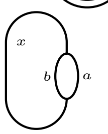
PROOF. We have the non-zero quantum trace for the left hand of the above if and only if $c = c'$ and $\mu = \mu'$. In this case we see

 $= \Theta(a,b,c) = \sqrt{d_a d_b d_c} = \sqrt{\frac{d_a d_b}{d_c}} d_c = \sqrt{\frac{d_a d_b}{d_c}}$  ,

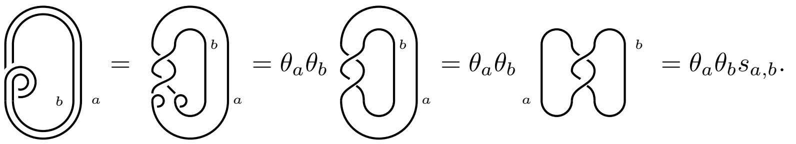
which implies the required formula. □

LEMMA 3.4. $$\theta_a \theta_b s_{a,b} = \operatorname{Tr} \theta_{a \otimes b} = \sum_x N_{a,b}^x \theta_x d_x .$$

PROOF. $\operatorname{Tr} \theta_{a\otimes b} =$  $= \sum_x \frac{N_{a,b}^x d_x}{\Theta(a,b,x)}$  $= \sum_x \frac{N_{a,b}^x d_x}{\Theta(a,b,x)}$ 

$= \sum_x \frac{N_{a,b}^x d_x \theta_x}{\Theta(a,b,x)}$  $= \sum_x \frac{N_{a,b}^x d_x \theta_x}{\Theta(a,b,x)} \Theta(a,b,x) = \sum_x N_{a,b}^x d_x \theta_x .$

On the other hand,



□

So we have the S-matrix formula:

Theorem 3.5 (**balancing equation**). $$s_{a,b} = \sum_x N_{ab}^x \frac{\theta_x}{\theta_a\theta_b} d_x.$$

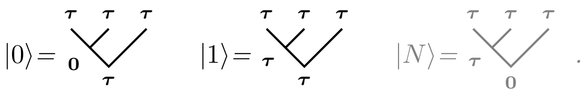
4. Fibonacci anyon and its braiding

Fibonacci anyon $\boldsymbol{\tau}$ is determined the following situation:

$$\mathcal{F} = \{\mathbf{0}, \boldsymbol{\tau}\}, \quad \tau \otimes \tau \to \mathbf{0} + \tau, \qquad N_{\boldsymbol{\tau}\boldsymbol{\tau}}^{\boldsymbol{\tau}} = 1,\ N_{\boldsymbol{\tau}\boldsymbol{\tau}}^{\mathbf{0}} = 1,\ N_{\boldsymbol{\tau}\mathbf{0}}^{\mathbf{0}} = 0.$$

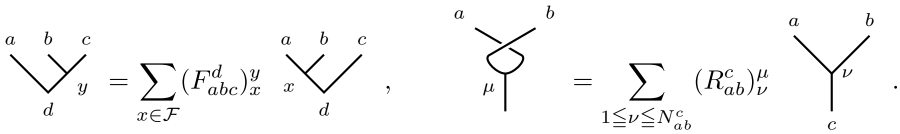
To consider the braiding matrices, we define the following vectors [6, 4]:

Definition 4.1. **fusion vectors** (**fusion trees, conformal blocks**)



The vector $|N\rangle$ is negligible since it plays the vacuum role. In the below, we discuss the 2-dimensional space for $|0\rangle$ and $|1\rangle$.

Now we define two matrices F, R as:



Then , by Mac Lane's coherence theorem [11], F-matrix satisfies the following equation:

Pentagon equation: $$(F_{12c}^5)_a^d (F_{a34}^5)_b^c = \sum_x (F_{234}^d)_x^c (F_{1x4}^5)_b^d (F_{123}^b)_a^x.$$

It is illustrated as:

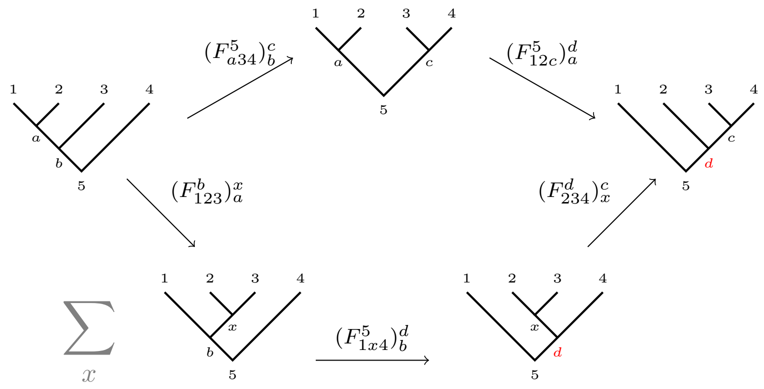


Figure 2. Pentagon axiom

By the above equation, we obtain F-matrix. For example, in the Fibonacci case, F acts on the space $V_{\mathbf{0}} \oplus V_{\boldsymbol{\tau}}$ and $F^{\boldsymbol{\tau}}_{\boldsymbol{\tau\tau\tau}} = \frac{1}{g}\begin{pmatrix} 1 & \sqrt{g} \\ \sqrt{g} & -1 \end{pmatrix}$ where $g = \frac{1+\sqrt{5}}{2}$ is the golden number.

Also, R-matrix satisfies the following equation:

Hexagon equation $$R^b_{13}(F^4_{213})^b_a R^a_{12} = \sum_x (F^4_{231})^b_x R^4_{1x} (F^4_{123})^x_a$$

It is expressed as:

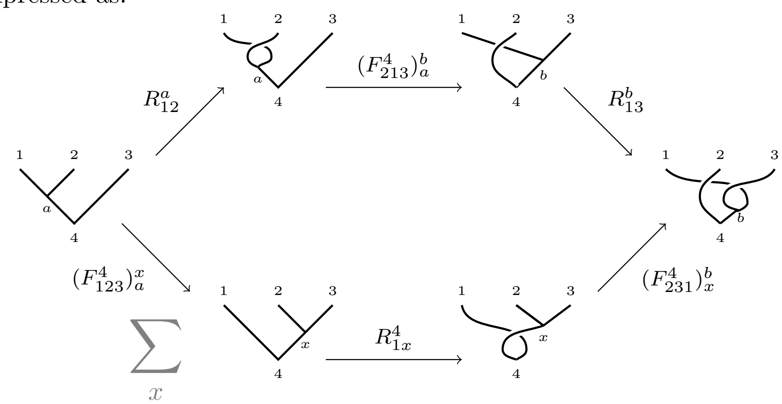
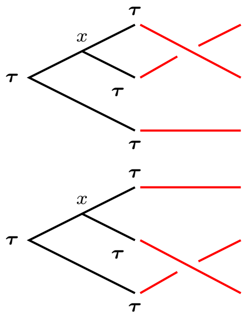


Figure 3. Hexagon axiom

For the Fibonacci, we have $R_{\boldsymbol{\tau\tau}} = \begin{pmatrix} R^{\mathbf{0}}_{\boldsymbol{\tau\tau}} & \\ 0 & R^{\boldsymbol{\tau}}_{\boldsymbol{\tau\tau}} \end{pmatrix} = \begin{pmatrix} e^{-\frac{4i\pi}{5}} & 0 \\ 0 & e^{\frac{3i\pi}{5}} \end{pmatrix}$ on $V_{\mathbf{0}} \oplus V_{\boldsymbol{\tau}}$.

So we define the **braiding matrices** B on the 2-dimensional space $\mathbb{C}|0\rangle \oplus \mathbb{C}|1\rangle$ by the following figure:



B_1: $R_{\tau\tau} = \mathrm{diag}(R^x_{\tau\tau})$ itself.

B_2: $\sum_y (F^{\tau}_{\tau\tau\tau})^x_y R^y_{\tau\tau} (F^{\tau}_{\tau\tau\tau})^y_x$: non-diagonal.

Figure 4. Braiding matrices

In this case, $B_1 = \begin{pmatrix} e^{-\frac{4i\pi}{5}} & 0 \\ 0 & e^{\frac{3i\pi}{5}} \end{pmatrix}$, $B_2 = \frac{1}{g}\begin{pmatrix} e^{\frac{4i\pi}{5}} & \sqrt{g}e^{-\frac{3i\pi}{5}} \\ \sqrt{g}e^{-\frac{3i\pi}{5}} & -1 \end{pmatrix}$.

5. Universal quantum gates

In quantum information theory, **1qubit** is 2-dimensional complex unit vector $\alpha|0\rangle + \beta|1\rangle \cong \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$ $(\,|\alpha|^2 + |\beta|^2 = 1)$. The quantum computer can be realized by the complicated circuits which are combinations of quantum gates. Typical 1qubit **quantum gates** are expressed by **Pauli matrices**:

$$\underset{\text{bit flip}}{X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}}, \qquad Y = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}, \qquad \underset{\text{phase flip}}{Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}}.$$

A typical 2-qubits quantum gate is **CNOT**(conditioned NOT) one

$$C_N = \begin{pmatrix} I & O \\ O & X \end{pmatrix} = P \otimes I + P^{\perp} \otimes X \qquad (P = |0\rangle\langle 0|,\ P^{\perp} = |1\rangle\langle 1|).$$

For any 1qubit $|x\rangle$, the CNOT gate works:

$$C_N\ |0\rangle \otimes |x\rangle = (P \otimes I)(|0\rangle \otimes |x\rangle) = |0\rangle \otimes |x\rangle$$
$$C_N\ |1\rangle \otimes |x\rangle = (P^{\perp} \otimes X)(|1\rangle \otimes |x\rangle) = |1\rangle \otimes X|x\rangle.$$

Thus, 1-st qubit is the **control** bit, which is not changed: For $|1\rangle$, the 2-nd qubit is changed by 'bit flip', and for $|0\rangle$ it is not changed.

If a set of quantum gates yields any other quantum one, it is called **universal set of gates**. It is known that the set of the gates

$$\underset{\text{Hadamard gate}}{\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}}, \qquad \underset{\frac{\pi}{8}\text{gate}}{\begin{pmatrix}e^{-\frac{i\pi}{8}} & 0\\ 0 & e^{\frac{i\pi}{8}}\end{pmatrix}}, \qquad \underset{\text{CNOT gate}}{\begin{pmatrix}I & O\\ O & X\end{pmatrix}} = \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}$$

is universal, see [13]. It is remarkable that the Fibonacci set of gates $\mathcal{B} = \{B_1, B_2\}$ is indeed universal, see [2]. It suffices to show that the CNOT gate can be approximated by combinations in $\mathcal{B}$.

First we give an approximation for iX:

$$\Phi(X): \; B_1^{-2}B_2^{-4}B_1^4B_2^{-2}B_1^2B_2^2B_1^{-2}B_2^4B_1^{-2}B_2^4B_1^2B_2^{-4}B_1^2B_2^{-2}B_1^2B_2^{-2}B_1^{-2} \approx iX$$

Next we give an approximation of the identity matrix which changes the string; it is used as 'injection' or 'ejection' of particles:

$$\Phi(I): \; B_1^3\,B_2^{-2}\,B_1^2\,B_2^2\,B_1^{-2}\,B_2^2\,B_1^4\,B_2^{-2}\,B_1^{-4}\,B_2^{-4}\,B_1^{-2}\,B_2^{-2}\,B_1^2\,B_2^4\,B_1^2\,B_2^{-4}\,B_1^{-2}\,B_2^3 \approx I$$

Combining these approximations, we obtain the CNOT approximately: $\Phi(I)^{-1}\Phi(X)\Phi(I)$.

As for a picture of a higher-oerder approximation of iX by Solovay-Kitaev, see [8], which is an improvement with an accuracy of $O(10^{-4})$.

Acknowledgements. This work was supported by Grant-in-Aid for Scientific Research (C), JSPS KAKENHI Grant Number JP 16K05253.

References

[1] B.Bakalov and A.Kirillov, "Lectures on Tensor Categories and Modular Functor", Amer. Math. Soc., 2000.

[2] N.Bonesteel, L.Hormozi, G.Zikos and S.H.Simon, Braid topologies for quantum computation, Phys. Rev. Lett., **95**(2005), 140503.

[3] G.P.Collins, Computing with Quantum Knots, Scientific American, April, 2006, 56–63.

[4] S.Eliëns, "Anyon Condensation", Master Thesis in Univ. Amsterdam 2010. `http://dare.uva.nl/document/206602`

[5] P.Etingof, S.Gelaki, D.Nikshych and V.Ostrik, "Tensor Categories", Math. Surveys and Mono. **205**, 2015, Amer. Math. Soc..

[6] J.I.Fujii, TQC in Fibonacci anyon (in Japanese), Osaka J. Math. Edu., **44**(2015), 151–164.

[7] J.I.Fujii, Modular S-matrix in TQC theory (in Japanese), Mem. Osaka Kyoiku Univ., **64/2**(2015), 15–33.

[8] L.Holmozi, "Topological Quantum Compiling", Thesis in Florida Univ., 2007.

[9] L.Hormozi, G.Zikos, E.Bonesteel and S.H.Simon, Topological quantum compiling, Phys. Rev. **B75**(2007), 165310.

[10] A.Kitaev, Anyons in an exactly solved model and beyond, Ann. of Phys., **321**(2006), 2–111.
[11] S.Mac Lane, "Categories for Working Mathematician" 2nd Ed., 1998, Springer.
[12] C.Nayak, S.H.Simon, A.Stern, M.Freedman and S.D.Sarma, Non-Abelian anyons and topological quantum computation, Rev. Modern Phys., **80**(2008), 1084–1159.
[13] M.A.Nielsen and I.L.Chuang, "Quantum Computation and Quantum Information", Cambridge Univ. Press, 2010.
[14] J.K.Pachos, "Introduction to Topological Quantum Computation", Cambridge, 2012.
[15] P.Panangaden and E.O.Paquette, A categorical presentation of quantum computation with anyons, in "New Structures for Physics", Lecture Notes in Physics **813**(2011), 983–1025.
[16] J.K.Slingerland and F.A.Bais, Quantum groups and non-abelian braiding in quantum hall systems, Nuc. Phys., **B612**(2001), 229–290.
[17] V.G.Turaev, "Quantum Invariants of Knots and 3-Manifolds, 2nd ed.", Walter de Gruyter Inc., 2010.
[18] Z.Wang, "Topological Quantum Computation", American Mathematical Society, 2008.

Jun Ichi FUJII

Department of Educational Collaboration (Science, Mathematics, Information), Osaka Kyoiku University, Asahigaoka, Kashiwara, Osaka 582-8582, Japan.
E-mail: fujii@cc.osaka-kyoiku.ac.jp