Quantum Information and Computation, Vol. 23, No. 7&8 (2023) 0541–0561
© Rinton Press

CRITERIA FOR ENTANGLEMENT AND SEPARABILITY OF DISCRETE QUANTUM STATES

MIAO WANG
Software Engineering Institute, East China Normal University, wmd0429@163.com
Shanghai 200062, China

ZHENFU CAO
Software Engineering Institute, East China Normal University, zfcao@sei.ecnu.edu.cn
Shanghai 200062, China
Research Center for Basic Theories of Intelligent Computing,
Research Institute of Basic Theories, Zhejiang Lab
Hangzhou 311121, China

XIAOLEI DONG[a]
Software Engineering Institute, East China Normal University, dongxiaolei@sei.ecnu.edu.cn
Shanghai 200062, China
Research Center for Basic Theories of Intelligent Computing,
Research Institute of Basic Theories, Zhejiang Lab
Hangzhou 311121, China

Received March 13, 2022
Revised April 18, 2023

Entanglement is an important quantum resource, which can be used in quantum teleportation and quantum computation. How to judge and measure entanglement or separability has become a basic problem in quantum information theory. In this paper, by analyzing the properties of generalized ring $\mathbb{Z}[i]^{2^n}$, a new method is presented to judge the entanglement or separability of any quantum state in the discrete quantum computing model proposed by Gatti and Lacalle. Different from previous criteria based on matrices, it is relatively simple to operate in mathematical calculation. And if a quantum state is separable, it can calculate the separable mathematical expression. Taking $n = 2, 3$ as examples, the concrete forms of all separable states in the model are presented. It provides a new research perspective for the discrete quantum computing model.

Keywords: Entangled states; Separable states; Discrete quantum states; The ring of Gaussian integers

1 Introduction

Quantum entangled state is a special kind of quantum state, but exists ubiquitous in the multipartite systems [1]. It is one of the wonderful properties of quantum mechanics, which enables quantum information to realize new functions that cannot be realized by classical information. As the carrier of quantum teleportation and quantum computation, entangled states are widely used in quantum cryptography [2], dense coding [3], quantum teleportation [4], quantum correction [5], fault-tolerant computing [6], large number factoring algorithm

[a] The corresponding author.

[7], Grover searching algorithm [8] and other fields. When a certain amount of entangled states are shared between the two places, the entangled owners can perform the functions of quantum teleportation and quantum computation by performing local operations on the entangled states and be supplemented by classical communication. The purpose of quantum information research is to develop and use entanglement to a great extent. Therefore, the study of quantum entanglement is of great significance to promote quantum informatics and has very important applications in some cutting-edge technologies.

Quantum entanglement is the inevitable result of quantum mechanics theory. The term "entanglement" can be traced back to the beginning of the birth of quantum mechanics. Historically, the cat paradox of Schrӧdinger [9] first proposed the concept of "entangled state", that is, the states of two entangled particles are interrelated and determined by each other. In 1935, Einstein, Podolsky and Rosen discovered the wonderful nonclassical property of entanglement [10], and they proposed the following quantum state

$$\Psi(x_1, x_2) = \int_{-\infty}^{+\infty} \exp\left[i/h\left(x_1 - x_2 + x_0\right)p\right] dp$$

where x_1, x_2 refer to the coordinates of two particles respectively. The basic feature of such a quantum state is that it cannot be written as the direct product of quantum states in the two subsystems, namely

$$\Psi(x_1, x_2) \neq \phi(x_1)\phi(x_2).$$

This property means that there is a kind of global state in the composite system, which can't be written as the direct product of quantum states of all the subsystems. This phenomenon is called entanglement. The debate on EPR paradox has prompted people to be more and more interested in the quantum entangled state. Physicists have studied it for more than half a century and derived a lot of research work: Bell inequality, Bell theory [11], etc. However, the clear definitions of entanglement and separability were not given until 1989 by R.F. Werner [1].

To deeply understand the entangled state, many efforts have been made and many good results have been obtained, including some effective criteria for entanglement of discrete variables. Some are easy to operate but not necessary and sufficient conditions for entanglement, and some are the opposite. For example, the positive partial transpose criterion [12, 13], the computable cross-norm or realignment criterion [14, 15], the permutation separability criteria [16, 17, 18], the criterion based on Bloch representations [19], the local uncertainty relations [20, 21, 22, 23], the covariance matrices approach [24], the entanglement witnesses [25, 26, 27, 28] and Bell type inequality [29, 30, 31], etc. In addition, the entanglement of quantum states has been studied from different angles. For general multipartite quantum systems, the reference [32] proposed using Pauli matrix to construct correlation tensor as the entanglement criterion. References [33] and [34] studied the entanglement of quantum states in multipartite systems by using invariants and the decomposition of matrix tensor product. Although many related results have been obtained, for any given quantum state, determining whether it is entangled or separable is still a very challenging and unsolved problem.

In 2018, Gatti and Lacalle proposed a model of discrete quantum computing [35], the set of Gaussian coordinate states. It includes all the quantum states whose coordinates in the computation base, except for a normalization factor $\sqrt{2}^{-k}$, belong to the ring of Gaussian integers $\mathbb{Z}[i] = \{a + ib | a, b \in \mathbb{Z}\}$. The model has the following properties: It describes real states in quantum physics, preserves the superposition and entanglement of quantum states and allows to approximate general quantum states, and, above all, it contains simple quantum states. For this model, we introduce a new method to judge entanglement and separability of quantum states. Compared with those classical methods, its operation is relatively simple.

In the first part of the paper, after establishing the required basic knowledge, we define a generalized ring of Gaussian integers $\mathbb{Z}[i]^{2^n}$ by analogy with the classical ring of Gaussian integers $\mathbb{Z}[i]$, and conjecture that the ring has similar properties to the classical ring, what's more, we can use these properties to explore entanglement and separability of quantum states in the model of Gatti and Lacalle.

In the second part, we prove some basic properties of the generalized ring $\mathbb{Z}[i]^{2^n}$, and verify our conjecture. That is, the ring has similar properties to the classical ring $\mathbb{Z}[i]$. It is a Euclidean domain, principal ideal domain and unique factorization domain. In addition, by analyzing the elements of the integer coordinate part and the complex coordinate part, all forms of prime elements and irreducible elements in the ring are discussed.

Finally, to go further with the analysis of elements in the extended ring $\mathbb{Z}[i]^{2^n}$, we find that the structure of elements in the ring is related to the entanglement and separability of quantum states in the discrete quantum model. By discussing prime elements and the number of prime elements of $\mathbb{Z}[i]$ contained in the coordinate states over the ring $\mathbb{Z}[i]^{2^n}$, we obtain a series of criteria for entangled states and separable states. Furthermore, by using the factorization property of the generalized ring, we show all types of separable states in the model when $n = 2, 3$, and assert that any quantum state can be compared with this method to judge its entanglement and separability in the n-qubits model. In Section 5, We provide a simple comparison for different methods.

2 Background knowledge

In this section, we will introduce some basic knowledge involved in this paper, including entangled states, separable states, discrete quantum models and the classical ring of Gaussian integers.

2.1 Entangled states and separable states

In quantum mechanics, the state of the system is expressed by wave function $|\psi\rangle$. There are two kinds of quantum states, pure states and mixed states. A quantum state that can be represented by a unit vector in Hilbert space is called *pure state*. The system cannot be described by a certain pure state, but needs to be described by a group of pure state vectors and their corresponding probabilities, so the quantum system is said to be in a *mixed state*. Pure states and mixed states can also be defined by density operator or density matrix.

Definition 2.1.1 Density matrix ρ is defined as a linear combination of a set of pure state ensemble $\{p_i, |\psi\rangle_i\}$ with certain probability, namely

$$\rho = \sum_i p_i \, |\psi\rangle_i \, \langle\psi|_i \, ,$$

where $\langle\psi|_i$ is the conjugate transpose of the state $|\psi\rangle_i$, and $p_i > 0, \sum_i p_i = 1$.

It means ρ is composed of a series of pure states $|\psi\rangle_i$ according to the probability p_i. Then it is easy to determine whether a given quantum state is pure or mixed by using density matrix. If $Tr\rho^2 = 1$, ρ is pure. If $Tr\rho^2 < 1$, ρ is mixed. When the system is in the exact known pure state $|\psi\rangle$, the density matrix is $\rho = |\psi\rangle \langle\psi|$.

Pure states can be classified into two types: separable pure states and entangled pure states. So are mixed states: separable mixed states and entangled mixed states.

We will first discuss the simple case of the pure state of a bipartite system.

Definition 2.1.2 [36] In a bipartite system $H_A \otimes H_B$, if the coherent superposition state $|\Psi\rangle_{AB}$ can be expressed as the tensor product of $|\psi\rangle_A$ and $|\psi\rangle_B$, namely

$$|\Psi\rangle_{AB} = |\psi\rangle_A \otimes |\psi\rangle_B ,$$

where $|\psi\rangle_A$ and $|\psi\rangle_B$ represent two pure states in Hilbert spaces H_A and H_B respectively. Then $|\Psi\rangle_{AB}$ is called separable.

If the quantum pure state $|\Psi\rangle_{AB}$ cannot be described as the tensor product of quantum states over the two subsystems, i.e. $|\Psi\rangle_{AB} \neq |\psi\rangle_A \otimes |\psi\rangle_B$, then the state $|\Psi\rangle_{AB}$ is entangled. For example, $\frac{1}{\sqrt{2}} \left(|0\rangle_A |1\rangle_B - |1\rangle_A |0\rangle_B\right)$ is a 2-qubits entangled state.

In a multipartite system $H_{ABC\cdots}$, if the pure state of multiple qubits $|\Psi\rangle_{ABC\cdots}$ can be expressed as

$$|\Psi\rangle_{ABC\cdots} = |\psi\rangle_A \otimes |\psi\rangle_B \otimes |\psi\rangle_C \otimes \cdots ,$$

where $|\Psi\rangle_{ABC\cdots} \in H_{ABC\cdots}, H_{ABC\cdots} = H_A \otimes H_B \otimes H_C \otimes \cdots , |\psi\rangle_A \in H_A, |\psi\rangle_B \in H_B, |\psi\rangle_C \in H_C, \cdots$, then $|\Psi\rangle_{ABC\cdots}$ is called separable state, otherwise it is entangled state.

The following is the definition of separability and entanglement of mixed states.

Definition 2.1.3 Suppose that ρ_{AB} is a density matrix in the bipartite system. If there are reduced density matrices ${\rho_i}^A$ of subsystem A and ${\rho_i}^B$ of subsystem B respectively, such that

$$\rho_{AB} = \sum_i p_i {\rho_i}^A \otimes {\rho_i}^B,$$

where ${\rho_i}^A = Tr_B(\rho_{AB}), {\rho_i}^B = Tr_A(\rho_{AB})$, Tr_B and Tr_A are operator maps. Then ρ_{AB} is separable. Otherwise ρ_{AB} is entangled.

In a multipartite system, the necessary and sufficient condition for being separable of density matrix ρ is that it can be written in the following form

$$\rho = \sum_i p_i {\rho_i}^1 \otimes {\rho_i}^2 \otimes \cdots {\rho_i}^k \otimes \cdots ,$$

where ${\rho_i}^k$ is the reduced density matrix with the probability p_i of the kth subsystem.

In this paper, we will discuss the separability or entanglement of states in the discrete quantum computing model proposed by Gatti and Lacalle.

2.2 ***Gatti*** & ***Lacalle discrete quantum computing model E***

In 2018, Gatti and Lacalle proposed a discrete quantum computing model, namely the set of Gaussian coordinate states E [35]. It is the smallest set of quantum states which contains a computational base and is invariant under the application of the conforming gates H and G.

Let H_2 be the state space of single qubit, which is a 2-dimensional Hilbert space,

$$|\psi\rangle_i = c_{i0}\,|0\rangle + c_{i1}\,|1\rangle \in H_2$$

is the ith qubit state, then the state with n-qubits composed of them is

$$|\psi\rangle = |\psi\rangle_1 \otimes |\psi\rangle_2 \otimes \cdots \otimes |\psi\rangle_n = \sum_{x=0}^{N-1} c_x\,|x\rangle\,.$$

Where $N = 2^n$ is the dimension of n-qubits state space $H_2{}^{\otimes} = H_2 \otimes H_2 \otimes \cdots \otimes H_2$.

Gatti and Lacalle showed that Gaussian integers are used to represent the coordinates of quantum states in the model. It is an important feature of this model.

The following is the 2^n-dimensional Gaussian integer vector set to be used in this paper,

$$\mathbb{Z}[i]^{2^n} = \{(x_0 + iy_0, \cdots, x_{2^n-1} + iy_{2^n-1})|x_i, y_i \in \mathbb{Z}, 0 \le i \le 2^n\}.$$

Definition 2.2.1 [35](Set of Gaussian coordinate states E) Let $|\psi\rangle$ be a quantum state. $|\psi\rangle \in E$ if and only if there exists $k \in N$ such that $\sqrt{2}^k\,|\psi\rangle \in \mathbb{Z}[i]^{2^n}$.

The set E can be written as the disjoint union of subsets of E, indexed by the parameter k. It is denoted by F_k:

$$F_k = \{|\psi\rangle \in E|\sqrt{2}^k\,|\psi\rangle \in \mathbb{Z}[i]^{2^n} and \sqrt{2}^{k-2}\,|\psi\rangle \notin \mathbb{Z}[i]^{2^n}\}.$$

The definition above can be rewritten in the following terms.

The state $|\psi\rangle$ of the form $|\psi\rangle = \frac{1}{\sqrt{2}^k}(x_0 + iy_0, \cdots, x_{2^n-1} + iy_{2^n-1})$ belongs to the level F_k if the following properties hold:

(i) $(x_0 + iy_0, \cdots, x_{2^n-1} + iy_{2^n-1}) \notin \mathbb{Z}[i]^{2^n}$.

(ii) $x_0{}^2 + \cdots + x_{2^n-1}{}^2 + y_0{}^2 + \cdots + y_{2^n-1}{}^2 = \sqrt{2}^k$.

(iii) $2 \nmid gcd(x_0, \cdots, x_{2^n-1}, y_0, \cdots, y_{2^n-1})$ (2 does not divide the greatest common divisor of $x_0, \cdots, x_{2^n-1}, y_0, \cdots, y_{2^n-1}$).

2.3 ***The ring of Gaussian integers*** $\mathbb{Z}[i]$

The number like $a + bi(a, b \in \mathbb{Z}, i = \sqrt{-1})$ is called Gaussian integer, which was proposed by Gauss when studying quadratic indefinite equation. Record as

$$\mathbb{Z}[i] = \{a + bi|a, b \in \mathbb{Z}, i = \sqrt{-1}\}.$$

For ordinary addition and multiplication, it can be proved that it is a domain, which we call the ring of Gaussian integers [37].

Property 2.3.1 It holds that

(i) $\mathbb{Z}[i]$ is a Euclidean domain.
(ii) $\mathbb{Z}[i]$ is a principal ideal domain.
(iii) $\mathbb{Z}[i]$ is a unique factorization domain.

Property 2.3.2 There are only four units $\pm 1, \pm i$ in $\mathbb{Z}[i]$.

Property 2.3.3 There are two types of prime elements in $\mathbb{Z}[i]$:

(i) $a^2 + b^2$ is a prime, then $a + bi$ is a prime element of $\mathbb{Z}[i]$.
(ii) p is a prime, $x^2 + y^2 = p$ has no integer solution, then $\pm p, \pm pi$ are prime elements of $\mathbb{Z}[i]$.

From the properties of the ring of Gaussian integers, we guess that there is a ring of multiple Gaussian integers, which has similar properties to the classical ring and is related to the Gaussian coordinate states. Fortunately, our conjecture has been verified in the following.

3 The ring of multiple Gaussian integers $\mathbb{Z}[i]^{2^n}$

In this section, we define "+" and "×" for the set

$$\mathbb{Z}[i]^{2^n} = \{(x_0 + iy_0, \cdots, x_{2^n-1} + iy_{2^n-1}) | x_t, y_t \in \mathbb{Z}, 0 \le t \le 2^n\}.$$

For $\alpha, \beta \in \mathbb{Z}[i]^{2^n}$, let

$$\alpha = (a_0 + ib_0, \cdots, a_{2^n-1} + ib_{2^n-1}),$$
$$\beta = (c_0 + id_0, \cdots, c_{2^n-1} + id_{2^n-1}).$$

We have

$$\alpha + \beta \triangleq (a_0 + ib_0 + c_0 + id_0, \cdots, a_{2^n-1} + ib_{2^n-1} + c_{2^n-1} + id_{2^n-1}),$$
$$\alpha \times \beta \triangleq ((a_0 + ib_0) \times (c_0 + id_0), \cdots, (a_{2^n-1} + ib_{2^n-1}) \times (c_{2^n-1} + id_{2^n-1})).$$

From the definition of the ring, it is easy to prove that $\mathbb{Z}[i]^{2^n}$ is a domain. Also, we will discuss the properties of $\mathbb{Z}[i]^{2^n}$. These properties will pave the way for the next exploration of the model.

For the sake of clarity in the structure of the paper, only the description of relevant properties is given below, and the detailed proof processes can be found in the Appendix A.

Property 3.1 $\mathbb{Z}[i]^{2^n}$ is a Euclidean domain.

Property 3.2 $\mathbb{Z}[i]^{2^n}$ is a principal ideal domain and unique factorization domain.

Property 3.3 There are 4^{2^n} units in $\mathbb{Z}[i]^{2^n}$.

The following discussion is about the prime elements for $\mathbb{Z}[i]^{2^n}$. The prime elements in the ring $\mathbb{Z}[i]^{2^n}$ can be divided into two parts. One part is that the components are all integers, and the other is that the components contain elements in the form of $a + bi (b \neq 0)$. We first discuss the prime elements whose components are all integers.

Obviously, because the prime elements require no other factors except itself and units, the elements containing composite numbers in the components must not be prime elements according to the definition of multiplication in the ring $\mathbb{Z}[i]^{2^n}$. Therefore, only elements without composite number components can be prime elements in $\mathbb{Z}[i]^{2^n}$. However, prime numbers are prime elements in the ring of integers $\mathbb{Z}$, but they are not necessarily prime elements in $\mathbb{Z}[i]$. For example, the prime number 2 can be decomposed into $2 = (1+i)(1-i)$ in $\mathbb{Z}[i]$, where 1±i are not trivial factors of 2. Therefore, 2 is not a prime element in $\mathbb{Z}[i]$. Generally, except the prime number 2, other prime numbers can be written in two forms, $4n+1$ and $4n+3$. Hence we have the following propositions.

Property 3.4 Let $p_i (0 \leq i \leq 2^n - 1)$ be a prime number. The equation $x^2 + y^2 = p_i$ has no integer solution if and only if the elements in the form of $(1, \cdots, 1, p_i, 1, \cdots, 1)$ are prime elements in $\mathbb{Z}[i]^{2^n}$.

Property 3.5 If the prime number $p_i (0 \leq i \leq 2^n - 1)$ can be written in the form of $4n+3$, then the elements shaped as $(1, \cdots, 1, p_i, 1, \cdots, 1)$ are prime elements in $\mathbb{Z}[i]^{2^n}$.

Property 3.6 If the prime number $p_i (0 \leq i \leq 2^n - 1)$ is in the form of $4n+1$, then the elements shaped as $(1, \cdots, 1, p_i, 1, \cdots, 1)$ are nonprime elements in $\mathbb{Z}[i]^{2^n}$.

Next, we will discuss the prime elements with the from $a + bi (b \neq 0)$ in components.

Property 3.7 Let $\alpha_j = a + bi, \alpha_j \notin \mathbb{Z}, \alpha_j \in \mathbb{Z}[i], 0 \leq j \leq 2^n - 1$. $a^2 + b^2$ is a prime number. Then the elements in the form of $(1, \cdots, 1, \alpha_j, 1, \cdots, 1)$ are prime elements in $\mathbb{Z}[i]^{2^n}$.

Property 3.8 Let $\alpha_j = a + bi, \alpha_j \notin \mathbb{Z}, \alpha_j \in \mathbb{Z}[i]$, $a^2 + b^2 = p_1 p_2 \cdots p_n$, where $p_t (1 \leq t \leq n)$ is a prime number. We have

(i) If $n = 1$, then the element in the form of $(1, \cdots, 1, \alpha_j, 1, \cdots, 1)$ is a prime element in $\mathbb{Z}[i]^{2^n}$.

(ii) If $n \neq 1$, then the element in the form of $(1, \cdots, 1, \alpha_j, 1, \cdots, 1)$ is a nonprime element in $\mathbb{Z}[i]^{2^n}$.

Property 3.9 If an element contains two or more components that are not 1, then the element is not a prime element in $\mathbb{Z}[i]^{2^n}$.

Property 3.10 An element in $\mathbb{Z}[i]^{2^n}$ is a prime element if and only if it is an irreducible element.

4 Criteria for entanglement or separability of quantum states in the model E

We have investigated the structure of the ring $\mathbb{Z}[i]^{2^n}$. Now we turn our attention to the quantum states in the model E proposed by Gatti and Lacalle. From Section 2.2, this discrete quantum computing model is the set of Gaussian coordinate states E. Let $|\psi\rangle$ be a quantum state, we have

$$E = \{|\psi\rangle \, |There\ exists\ k \in N\ such\ that\ \sqrt{2}^k \, |\psi\rangle \in \mathbb{Z}[i]^{2^n}\}.$$

Hence, judging the entanglement or separability of the state $|\psi\rangle$ in E is the same as judging the entanglement or the separability of $\sqrt{2}^k \, |\psi\rangle$.

According to Property 3.2, the ring $\mathbb{Z}[i]^{2^n}$ has the unique factorization property. Each element that is neither zero nor unit can be uniquely factorized into the product of some prime elements. Assuming that A is a non-zero and non-unit element in $\mathbb{Z}[i]^{2^n}$, it can be decomposed into:

$$A = P_1 P_2 P_3 \cdots P_r,$$

P_i is a prime element in $\mathbb{Z}[i]^{2^n}$. From the properties in Section 3, $P_i = (1, \cdots, 1, p_j, 1, \cdots, 1)$, where p_j is a prime element in $\mathbb{Z}[i]$. By simple deformation, A can also be uniquely expressed as

$$A = (p_{1,1} p_{1,2} \cdots p_{1,k_1}, p_{2,1} p_{2,2} \cdots p_{2,k_2}, \cdots, p_{r,1} p_{r,2} \cdots p_{r,k_r}),$$

where $p_{i,j}$ is a prime element in $\mathbb{Z}[i]$. Then do the combination calculation, if there is a combination about $p_{i,j}$ that can write A as a tensor product, then the corresponding quantum state is separable, otherwise it is entangled. If it is separable, then the tensor product is the separable mathematical expression of the quantum state.

From the properties obtained in Section 3, the following are some criteria of separability or entanglement. Finally, using the unique factorization property and combination calculation, we present all types of separable states and their representations for $n = 2, 3$.

Property 4.1 Let $|\psi\rangle$ be a quantum state, $|\psi\rangle \in E$. If $\sqrt{2}^k \, |\psi\rangle$ is a prime element in $\mathbb{Z}[i]^{2^n}$, then $|\psi\rangle$ is an entangled state.

Proof: Let $|\psi\rangle = \frac{1}{\sqrt{2}^k}(x_0 + iy_0, \cdots, x_{2^n-1} + iy_{2^n-1})$, then $\sqrt{2}^k \, |\psi\rangle = (x_0 + iy_0, \cdots, x_{2^n-1} + iy_{2^n-1}) \in \mathbb{Z}[i]^{2^n}$. Since $\sqrt{2}^k \, |\psi\rangle$ is a prime element in $\mathbb{Z}[i]^{2^n}$, from Proposition 3.10, we have that $\sqrt{2}^k \, |\psi\rangle$ is irreducible in $\mathbb{Z}[i]^{2^n}$. That is, there is no nontrivial factor. And then the quantum state $|\psi\rangle$ cannot be expressed in the form of tensor product of subsystems. Thus $|\psi\rangle$ is an entangled state □.

Property 4.2 A quantum state of the form $\frac{1}{\sqrt{2}^k}(q_0, \cdots, q_i, 1, \cdots, 1)$, where i is an even number and q_i is a prime element in $\mathbb{Z}[i]$, must be entangled.

Proof: Suppose that $\frac{1}{\sqrt{2}^k}(q_0, \cdots, q_i, 1, \cdots, 1)$ is a separable state, then it can be expressed as the tensor product of quantum states from n single quantum systems. Since q_i is a prime element in $\mathbb{Z}[i]$, only one subquantum state whose component contains q_i in the tensor product. Let

$$\begin{aligned}\frac{1}{\sqrt{2}^k}(q_0, \cdots, q_i, 1, \cdots, 1) &= |\psi\rangle_0 \otimes |\psi\rangle_1 \otimes \cdots \otimes |\psi\rangle_{n-1} \\ &= (a_{0,0}, a_{0,1}) \otimes (a_{1,0}, a_{1,1}) \otimes \cdots \otimes (a_{n-1,0}, a_{n-2,1}) \,.\end{aligned}$$

Suppose that $(a_{j,0}, a_{j,1})$ is the subquantum state. According to the definition of tensor product, there are even components with q_i in the composite quantum state. It contradicts the odd number of components with prime element in the proposition □.

Corollary 4.1 In Proposition 4.2, the conclusion is still valid when q_i is a reducible element.

Proof: When q_i is reducible in $\mathbb{Z}[i]$, the proof is similar to Proposition 4.1. We don't repeat it here □.

Property 4.3 A quantum state like $\frac{1}{\sqrt{2}^k}(q, \cdots, q, 1, \cdots, 1)$ is a separable state, where q is a prime element in $\mathbb{Z}[i]$ and the number of q in the quantum state is 2^{n-1}. Especially, $\frac{1}{\sqrt{2}^k}(q, \cdots, q)$ is a separable state.

Proof: For $\frac{1}{\sqrt{2}^k}(q, \cdots, q, 1, \cdots, 1)$ and $\frac{1}{\sqrt{2}^k}(q, \cdots, q)$, we have

$$\frac{1}{\sqrt{2}^k}(q, \cdots, q, 1, \cdots, 1) = \frac{1}{\sqrt{2}^k}(q, 1) \otimes (1, 1) \otimes \cdots \otimes (1, 1),$$
$$\frac{1}{\sqrt{2}^k}(q, \cdots, q) = \frac{1}{\sqrt{2}^k}(q, q) \otimes (1, 1) \otimes \cdots \otimes (1, 1).$$

Hence the two kinds of quantum states are separable □.

Corollary 4.2 In Proposition 4.3, the conclusion is still valid when q is a reducible element.

Proof: When q is reducible, the above two equations still hold □.

Property 4.4 Let $|\psi\rangle = \frac{1}{\sqrt{2}^k}(a_0, a_1, \cdots, a_{2^n-1})$, $|\psi\rangle \in E$, $\sqrt{2}^k |\psi\rangle \in \mathbb{Z}[i]^{2^n}$, where $a_i(i = 1, 2, \cdots, n)$ is 1 or a prime element in $\mathbb{Z}[i]$. Except the two types of quantum states in Proposition 4.2 and the quantum state $\frac{1}{\sqrt{2}^k}(1, \cdots, 1)$, other quantum states in the form of $|\psi\rangle$ are all entangled states.

Proof: When the components of the quantum state $|\psi\rangle$ contain odd prime elements in $\mathbb{Z}[i]$, by Proposition 4.2, $|\psi\rangle$ is an entangled state. When the number is even, suppose that $|\psi\rangle$ is a separable state. Then it can be expressed as the tensor product

$$|\psi\rangle = |\psi\rangle_0 \otimes |\psi\rangle_1 \otimes \cdots \otimes |\psi\rangle_{n-1} = (a_{0,0}, a_{0,1}) \otimes (a_{1,0}, a_{1,1}) \otimes \cdots \otimes (a_{n-1,0}, a_{n-2,1}).$$

Because a_i is 1 or a prime element in $\mathbb{Z}[i]$ and the number of prime elements is even, there are only $\frac{1}{\sqrt{2}^k}(q, \cdots, q, 1, \cdots, 1)$ and $\frac{1}{\sqrt{2}^k}(q, \cdots, q)$. The proposition is proved □.

By analyzing the relationship between the ring of multiple Gaussian integers and the set of Gaussian coordinate states and using the property that the ring is a unique factorization domain, we classify the number of reducible elements in $\mathbb{Z}[i]$ for the Gaussian coordinate states, and give all types of separable states in the model when $n = 2, 3$. Note that it doesn't consider the order of coordinates here. Let the number of reducible elements be t. We obtain

Case 1: When $n = 2$, all types of separable states in the model are as follows.

When $t = 0$, there are three types of separable states.

(i) p_1, q_1 are all prime elements in $\mathbb{Z}[i]$,

$$\frac{1}{\sqrt{2}^k}(p_1, p_1, q_1, q_1) = \frac{1}{\sqrt{2}^k}(p_1, q_1) \otimes (1, 1).$$

(ii) p_1 is a prime element in $\mathbb{Z}[i]$.

$$\frac{1}{\sqrt{2}^k}(p_1, p_1, 1, 1) = \frac{1}{\sqrt{2}^k}(p_1, 1) \otimes (1, 1).$$

(iii)

$$\frac{1}{\sqrt{2}^k}(1, 1, 1, 1) = \frac{1}{\sqrt{2}^k}(1, 1) \otimes (1, 1).$$

When $t = 1$, the type of separable states is the following.

(i) p_1, p_2 are all prime elements in $\mathbb{Z}[i]$,

$$\frac{1}{\sqrt{2}^k}(p_1p_2, p_1, p_2, 1) = \frac{1}{\sqrt{2}^k}(p_1, 1) \otimes (p_2, 1).$$

When $t = 2$, the separable states have the following types.

(i) p_1, q_1 are all prime elements in $\mathbb{Z}[i]$,

$$\frac{1}{\sqrt{2}^k}(p_1p_2, p_1, q_1p_2, q_1) = \frac{1}{\sqrt{2}^k}(p_1, q_1) \otimes (p_2, 1).$$

(ii) One of p_1 and p_2 is a prime element in $\mathbb{Z}[i]$, and the other is a reducible element,

$$\frac{1}{\sqrt{2}^k}(p_1p_2, p_1, p_2, 1) = \frac{1}{\sqrt{2}^k}(p_1, 1) \otimes (p_2, 1).$$

(iii) One of p_1 and q_1 is a prime element in $\mathbb{Z}[i]$, and the other is a reducible element,

$$\frac{1}{\sqrt{2}^k}(p_1, p_1, q_1, q_1) = \frac{1}{\sqrt{2}^k}(p_1, q_1) \otimes (1, 1).$$

(iv) p_1 is a reducible element in $\mathbb{Z}[i]$,

$$\frac{1}{\sqrt{2}^k}(p_1, p_1, 1, 1) = \frac{1}{\sqrt{2}^k}(p_1, 1) \otimes (1, 1).$$

When $t = 3$, the separable states have the following types.

(i) One of p_1 and q_1 is a prime element in $\mathbb{Z}[i]$, and the other is a reducible element,

$$\frac{1}{\sqrt{2}^k}(p_1p_2, p_1, q_1p_2, q_1) = \frac{1}{\sqrt{2}^k}(p_1, q_1) \otimes (p_2, 1).$$

(ii) p_1, p_2 are all reducible elements in $\mathbb{Z}[i]$,

$$\frac{1}{\sqrt{2}^k}(p_1p_2, p_1, p_2, 1) = \frac{1}{\sqrt{2}^k}(p_1, 1) \otimes (p_2, 1).$$

When $t = 4$, the separable states have the following types.

(i) p_1, p_2, q_1, q_2 can be prime elements or reducible elements in $\mathbb{Z}[i]$,

$$\frac{1}{\sqrt{2}^k}(p_1p_2, p_1q_2, q_1p_2, q_1q_2) = \frac{1}{\sqrt{2}^k}(p_1, q_1) \otimes (p_2, q_2).$$

(ii) p_1, q_1 are all reducible elements in $\mathbb{Z}[i]$,

$$\frac{1}{\sqrt{2}^k}(p_1p_2, p_1, q_1p_2, q_1) = \frac{1}{\sqrt{2}^k}(p_1, q_1) \otimes (p_2, 1).$$

(iii) p_1, q_1 are all reducible elements in $\mathbb{Z}[i]$,

$$\frac{1}{\sqrt{2}^k}(p_1, p_1, q_1, q_1) = \frac{1}{\sqrt{2}^k}(p_1, q_1) \otimes (1, 1).$$

Case 2: When $n = 3$, all types of separable states in the model are as follows.

When $t = 0$, the separable states have the following types.

(i) p_1 is a prime element in $\mathbb{Z}[i]$,

$$\frac{1}{\sqrt{2}^k}(p_1, p_1, p_1, p_1, 1, 1, 1, 1) = \frac{1}{\sqrt{2}^k}(p_1, 1) \otimes (1, 1) \otimes (1, 1).$$

(ii) p_1, q_1 are all prime elements in $\mathbb{Z}[i]$,

$$\frac{1}{\sqrt{2}^k}(p_1, p_1, p_1, p_1, q_1, q_1, q_1, q_1) = \frac{1}{\sqrt{2}^k}(p_1, q_1) \otimes (1, 1) \otimes (1, 1).$$

(iii)

$$\frac{1}{\sqrt{2}^k}(1, 1, 1, 1, 1, 1, 1, 1) = \frac{1}{\sqrt{2}^k}(1, 1) \otimes (1, 1) \otimes (1, 1).$$

When $t=1$, there is no separable state.

When $t=2$, the type of separable states is the following.

(i) p_1, p_2 are all prime elements in $\mathbb{Z}[i]$,

$$\frac{1}{\sqrt{2}^k}(p_1p_2, p_1p_2, p_1, p_1, p_2, p_2, 1, 1) = \frac{1}{\sqrt{2}^k}(p_1, 1)\otimes(p_2, 1)\otimes(1, 1).$$

When $t=3$, there is no separable state.

When $t=4$, the separable states have the following types.

(i) One of p_1 and q_1 is a prime element in $\mathbb{Z}[i]$, and the other is a reducible element,

$$\frac{1}{\sqrt{2}^k}(p_1, p_1, p_1, p_1, q_1, q_1, q_1, q_1) = \frac{1}{\sqrt{2}^k}(p_1, q_1)\otimes(1, 1)\otimes(1, 1).$$

(ii) p_1 is a reducible element in $\mathbb{Z}[i]$,

$$\frac{1}{\sqrt{2}^k}(p_1, p_1, p_1, p_1, 1, 1, 1, 1) = \frac{1}{\sqrt{2}^k}(p_1, 1)\otimes(1, 1)\otimes(1, 1).$$

(iii) One of p_1 and p_2 is a prime element in $\mathbb{Z}[i]$, and the other is a reducible element,

$$\frac{1}{\sqrt{2}^k}(p_1p_2, p_1p_2, p_1, p_1, p_2, p_2, 1, 1) = \frac{1}{\sqrt{2}^k}(p_1, 1)\otimes(p_2, 1)\otimes(1, 1).$$

(iv) p_1, q_1 are all prime elements in $\mathbb{Z}[i]$,

$$\frac{1}{\sqrt{2}^k}(p_1p_2, p_1p_2, p_1, p_1, q_1p_2, q_1p_2, q_1, q_1) = \frac{1}{\sqrt{2}^k}(p_1, q_1)\otimes(p_2, 1)\otimes(1, 1).$$

(v) p_1, p_2, p_3 are all prime elements in $\mathbb{Z}[i]$,

$$\frac{1}{\sqrt{2}^k}(p_1p_2p_3, p_1p_2, p_1p_3, p_1, p_2p_3, p_2, p_3, 1) = \frac{1}{\sqrt{2}^k}(p_1, 1)\otimes(p_2, 1)\otimes(p_3, 1).$$

When $t=5$, the type of separable states is the following.

(i) There is only one prime element among p_1, p_2, p_3 in $\mathbb{Z}[i]$,

$$\frac{1}{\sqrt{2}^k}(p_1p_2p_3, p_1p_2, p_1p_3, p_1, p_2p_3, p_2, p_3, 1) = \frac{1}{\sqrt{2}^k}(p_1, 1)\otimes(p_2, 1)\otimes(p_3, 1).$$

When $t=6$, the separable states have the following types.

(i) p_1, p_2 are all reducible elements in $\mathbb{Z}[i]$,

$$\frac{1}{\sqrt{2}^k}(p_1p_2, p_1p_2, p_1, p_1, p_2, p_2, 1, 1) = \frac{1}{\sqrt{2}^k}(p_1, 1) \otimes (p_2, 1) \otimes (1, 1).$$

(ii) One of p_1 and q_1 is a prime element in $\mathbb{Z}[i]$, and the other is a reducible element,

$$\frac{1}{\sqrt{2}^k}(p_1p_2, p_1p_2, p_1, p_1, q_1p_2, q_1p_2, q_1, q_1) = \frac{1}{\sqrt{2}^k}(p_1, q_1) \otimes (p_2, 1) \otimes (1, 1).$$

(iii) There are two reducible elements among p_1, p_2, p_3 in $\mathbb{Z}[i]$,

$$\begin{aligned} &\frac{1}{\sqrt{2}^k}(p_1p_2p_3, p_1p_2, p_1p_3, p_1, p_2p_3, p_2, p_3, 1) \\ =&\frac{1}{\sqrt{2}^k}(p_1, 1) \otimes (p_2, 1) \otimes (p_3, 1). \end{aligned}$$

(iv) p_1, q_1 are all prime elements in $\mathbb{Z}[i]$,

$$\begin{aligned} &\frac{1}{\sqrt{2}^k}(p_1p_2p_3, p_1p_2, p_1p_3, p_1, q_1p_2p_3, q_1p_2, q_1p_3, q_1) \\ =&\frac{1}{\sqrt{2}^k}(p_1, q_1) \otimes (p_2, 1) \otimes (p_3, 1). \end{aligned}$$

When $t = 7$, the separable states have the following types.

(i) p_1, p_2, p_3 are all reducible elements in $\mathbb{Z}[i]$,

$$\begin{aligned} &\frac{1}{\sqrt{2}^k}(p_1p_2p_3, p_1p_2, p_1p_3, p_1, p_2p_3, p_2, p_3, 1) \\ =&\frac{1}{\sqrt{2}^k}(p_1, 1) \otimes (p_2, 1) \otimes (p_3, 1). \end{aligned}$$

(ii) One of p_1 and q_1 is a prime element in $\mathbb{Z}[i]$, and the other is a reducible element,

$$\begin{aligned} &\frac{1}{\sqrt{2}^k}(p_1p_2p_3, p_1p_2, p_1p_3, p_1, q_1p_2p_3, q_1p_2, q_1p_3, q_1) \\ =&\frac{1}{\sqrt{2}^k}(p_1, q_1) \otimes (p_2, 1) \otimes (p_3, 1). \end{aligned}$$

When $t = 8$, the separable states have the following types.

(i) p_1, q_1 are all reducible elements in $\mathbb{Z}[i]$,

$$\frac{1}{\sqrt{2}^k}(p_1, p_1, p_1, p_1, q_1, q_1, q_1, q_1) = \frac{1}{\sqrt{2}^k}(p_1, q_1) \otimes (1, 1) \otimes (1, 1).$$

(ii) p_1, q_1 are all reducible elements in $\mathbb{Z}[i]$,

$$\begin{aligned}&\frac{1}{\sqrt{2}^k}(p_1p_2, p_1p_2, p_1, p_1, q_1p_2, q_1p_2, q_1, q_1)\\=&\frac{1}{\sqrt{2}^k}(p_1, q_1)\otimes(p_2, 1)\otimes(1, 1).\end{aligned}$$

(iii) p_1, q_1 are all reducible elements in $\mathbb{Z}[i]$,

$$\begin{aligned}&\frac{1}{\sqrt{2}^k}(p_1p_2p_3, p_1p_2, p_1p_3, p_1, q_1p_2p_3, q_1p_2, q_1p_3, q_1)\\=&\frac{1}{\sqrt{2}^k}(p_1, q_1)\otimes(p_2, 1)\otimes(p_3, 1).\end{aligned}$$

(iv) p_1, p_2, q_1, q_2 can be prime elements or reducible elements in $\mathbb{Z}[i]$,

$$\begin{aligned}&\frac{1}{\sqrt{2}^k}(p_1p_2, p_1p_2, p_1q_2, p_1q_2, q_1p_2, q_1p_2, q_1q_2, q_1q_2)\\=&\frac{1}{\sqrt{2}^k}(p_1, q_1)\otimes(p_2, q_2)\otimes(1, 1).\end{aligned}$$

(v) p_1, p_2, p_3, q_1, q_2 can be prime elements or reducible elements in $\mathbb{Z}[i]$,

$$\begin{aligned}&\frac{1}{\sqrt{2}^k}(p_1p_2p_3, p_1p_2, p_1q_2p_3, p_1q_2, q_1p_2p_3, q_1p_2, q_1q_2p_3, q_1q_2)\\=&\frac{1}{\sqrt{2}^k}(p_1, q_1)\otimes(p_2, q_2)\otimes(p_3, 1).\end{aligned}$$

(vi) $p_1, p_2, p_3, q_1, q_2, q_3$ can be prime elements or reducible elements in $\mathbb{Z}[i]$,

$$\begin{aligned}&\frac{1}{\sqrt{2}^k}(p_1p_2p_3, p_1p_2q_3, p_1q_2p_3, p_1q_2q_3, q_1p_2p_3, q_1p_2q_3, q_1q_2p_3, q_1q_2q_3)\\=&\frac{1}{\sqrt{2}^k}(p_1, q_1)\otimes(p_2, q_2)\otimes(p_3, q_3).\end{aligned}$$

Note that $p_1, p_2, p_3, q_1, q_2, q_3$ are prime elements or reducible elements in $\mathbb{Z}[i]$.

To sum up, for the general n-qubits Gatti & Lacalle discrete quantum computing model E, we can assert that any quantum state can be judged its entanglement or separability by the unique factorization property of the ring $\mathbb{Z}[i]^{2^n}$. Only the bigger the n is, the more complicated the situation becomes.

5 Comparisons of different criteria

Now there are many separability criteria, but there is no universal method to determine whether a quantum state is separable or entangled. There are some classical criteria for quantum entanglement in discrete quantum state systems. For example, the positive partial transpose criterion [12, 13], the computable cross-norm or realignment criterion [14, 15], the permutation separability criterion [16, 17, 18], the covariance matrices criterion [24], the entanglement witnesses [25, 26, 27, 28] criterion and Bell type inequality criterion [29, 30, 31], etc. However, they are all used to determine whether a quantum state is separable or entangled, and do not give the decomposition formula of a separable quantum state in mathematics. The following briefly describes these determination methods and their scope of use.

The positive partial transpose criterion is only applicable to bipartite quantum states and a necessary condition for the separation of quantum states. It can be expressed as: if a bipartite state ρ_{AB} is separable, then the new matrix $\rho_{AB}^{T_B}$ formed by partial transposition of B system about the density matrix ρ_{AB} must satisfy inequality

$$\left\|\rho_{AB}^{T_B}\right\| \leq 1,$$

where $\|\cdot\|$ is the trace norm, and $\|A\| = Tr\sqrt{AA^{\dagger}}$.

The computable cross-norm criterion is also called realignment criterion. It is very similar to the positive partial transpose criterion. It describes: if a bipartite state ρ_{AB} is separable, then the new matrix $R(\rho_{AB})$ formed by realigning the indices of the density matrix ρ_{AB} must satisfy inequality

$$\|R(\rho_{AB})\| \leq 1,$$

where R is the realignment operation. This criterion is usually regarded as a supplement to the positive partial transpose criterion, but both them are the bipartite state criteria.

The permutation separability criterion actually covers the positive partial transpose criterion and the computable cross-norm criterion, and is applicable to the multipartite system. Take the example of the 3-partite system to show how this criterion works. If a 3-partite state ρ_{ABC} is separable, then the new matrix $L(\rho_{ABC})$ formed by swapping arbitrary indices of the density matrix ρ_{ABC} must satisfy inequality

$$\|L(\rho_{ABC})\| \leq 1,$$

where L refers to any index exchange operation.

In fact, all of these permutation criteria can only determine complete separability, that is, they can only tell us that a quantum state is completely separable or not, and no further information can be obtained. Moreover, the entanglement detection of multipartite system is a complex problem, and many separability criteria applicable to multipartite system are not simple, or even difficult to calculate, without operability.

The covariance matrices criterion also applies only to bipartite quantum states. It is relatively computationally complex. First, define the covariance matrix. If ρ_{AB} is a given quantum state, and $\{M_k : k = 1, \cdots, N\}$ is the observed measurement, then the $N \times N$ covariance matrix R is defined as:

$$\gamma_{i,j} = (\langle M_i M_j\rangle + \langle M_j M_i\rangle)/2 - \langle M_i\rangle \langle M_j\rangle .$$

If choose $\{M_k\} = \{A_k \otimes I, I \otimes B_k\}$ and the Hilbert-Schmidt orthogonal basis $\{A_k\}(\{B_k\})$ based on the operator space $\mathcal{H}_A(\mathcal{H}_B)$, then the covariance matrix has the following block structure,

$$\gamma(\rho_{AB}, \{M_k\}) = \begin{bmatrix} A & B \\ C^T & D \end{bmatrix},$$

where $A = \gamma(\rho_{AB}, \{A_k\})$ and $B = \gamma(\rho_{AB}, \{B_k\})$ are covariance matrices of reduced density matrices, and matrix C is composed of $C_{i,j} = \langle A_i \otimes B_j \rangle - \langle A_i \rangle \langle B_j \rangle$. The covariance matrices criterion is defined as: if a bipartite state ρ_{AB} is separable, there must be states $|a_k\rangle \langle a_k| (|b_k\rangle \langle b_k|)$ and weight coefficients p_k satisfying $\kappa_A = \sum_k p_k \gamma(|a_k\rangle \langle a_k|)(\kappa_B = \sum_k p_k \gamma(|b_k\rangle \langle b_k|))$. Then the following inequality holds

$$\gamma(\rho_{AB}, \{M_k\}) \geq \kappa_A \otimes \kappa_B.$$

otherwise ρ_{AB} is entangled.

Entanglement witnesses is a good tool for detecting entanglement in experiments. Theoretically, there is an entanglement witness for any entangled state, but the construction of entanglement witness is not an easy task. The idea comes from geometry and Hahn. Banach theorem, that is, the convex closed set and a point outside the set always have a hyperplane to divide the two. For example, if the entangled witness operator W is constructed, for any quantum state ρ, if

$$Tr(W\rho) \geq 0,$$

Then the quantum state ρ is determined as separable state by W, otherwise it is entangled state.

Bell-type inequality is also an effective tool for detecting entanglement in experiments. The violation of Bell inequality shows that the state is entangled. The basic idea of Bell inequality is as follows: When measuring a bipartite system, it is assumed that there is a measurement result locally on each side before the measurement, and then a quantitative limit of the correlation degree of the results when two associated particles are measured at the same time can be obtained. But it is not easy to use in practice, and the measurement process cannot simply measure preexisting local results.

The above are the criteria for judging entanglement or separability of quantum states under different conditions. At present, there is no universal separability criterion for either bipartite system or multipartite system. Each method has specific limitations. And they can only judge whether a quantum state is entangled or separable. When a quantum state is separable, they cannot give a specific mathematical separable expression.

By analyzing the properties of the ring $\mathbb{Z}[i]^{2^n}$, we find that it has a subtle relationship with Gatti & Lacale discrete quantum computing model E. If $|\psi\rangle \in E$, there exists $k \in N$ such that $\sqrt{2}^k |\psi\rangle \in \mathbb{Z}[i]^{2^n}$. We can use the unique factorization property of the ring $\mathbb{Z}[i]^{2^n}$ to judge the entanglement or separability. That is, each element $A \in \mathbb{Z}[i]^{2^n}$ which is neither zero nor unit can be uniquely factorized into the product of some prime elements,

$$A = P_1 P_2 P_3 \cdots P_r,$$

where P_i is a prime element in $\mathbb{Z}[i]^{2^n}$. By simply deforming A, it can be uniquely expressed as

$$A = (p_{1,1}p_{1,2} \cdots p_{1,k_1}, p_{2,1}p_{2,2} \cdots p_{2,k_2}, \cdots, p_{r,1}p_{r,2} \cdots p_{r,k_r}),$$

where $p_{i,j}$ is a prime element in $\mathbb{Z}[i]$. Through combination calculation, if there is a combination about $p_{i,j}$ that can write A as a tensor product, then the corresponding quantum state is separable, otherwise it is entangled. If it is separable, then the tensor product is the separable mathematical expression of the quantum state. Different from the previous criteria based on matrices, this method is relatively simple to operate in mathematics. But, at present, it is only valid for the discrete quantum model proposed by Gatti and Lacale. It is still an open problem for the general criterion.

6 Conclusions

Quantum entanglement is an arduous and challenging research. Some remarkable achievements have been made, but quantum entanglement still has many problems to be further studied.

In this paper, we present a new judgment method of entanglement and separability for the discrete quantum computing model proposed by Gatti and Lacalle. It is relatively simpler than previous methods in mathematical calculation. We find that the properties of quantum states are related to the Euclidean domain $\mathbb{Z}[i]^{2^n}$ in the model. Using the factorization property of the ring, a series of criteria are verified. In addition, we present all types of separable states when $n = 2, 3$, and assert that any quantum state can be compared with this method to determine entanglement or separability in the n-qubits model. From the perspective of quantum communication, the proposed method is significative. It provides a novel way to study the entanglement and separability of discrete quantum states.

Acknowledgements

This work is supported in part by the National Key Research and Development Program of China under Grant 2022YFB2701400, in part by the National Natural Science Foundation of China under Grant 62132005, Grant 62172161, Grant 62172162, and in part by Natural Science Foundation of Shanghai under Grant 20ZR1418400.

References

1. R. F. Werner (1989), *Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model*, Phys. Rev. A. Vol 40, 4277-4281.
2. A. K. Ekert (1991), *Quantum cryptography based on Bell's theorem*, Phys. Rev. Lett. Vol 67, 661–663.
3. K. Mattle, H. Weinfurter, P. G. Kwiat and A. Zeilinger (1996), *Dense coding in experimental quantum communication*, Phys Rev Lett. Vol 76, 4656–4659.
4. C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres and W. K. Wootters (1991), *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels*, Phys Rev Lett. Vol 67, 661–663.
5. J. Kempe (2007), *Quantum Decoherence*, Springer, Berlin.
6. A. Steane (1998), *Quantum computing. Reports on Progress in Physics*, Vol 61, 117–173.
7. A. Ekert and R. Jozsa (1996), *Quantum computation and Shor's factoring algorithm*, Reviews of Modern Physics, Vol 68, 733–753.
8. L. K. Grover (1997), *Quantum mechanics helps in searching for a needle in a haystack*, Phys Rev Lett. Vol 79, 325–328.
9. E. Schrödinger (1935), *Die gegenwärtige Situation in der Quantenmechanik*, Naturwissenschaften, Vol 23, 807-812.

10. A. Einstein, B. Podolsky and N. Rosen (1935), *Can quantum-mechanical description of physical reality be considered complete?* Phys. Rev. Vol 47, 777-780.
11. J. S. Bell (1964), *On the einstein-podolsky-rosen paradox*, Physics, Vol 1, 195–200.
12. S. BeigI and P. W. Shor (2010), *Approximating the set of separable states using the positive partial transpose test. Journal of Mathematical Physics*, Vol 51, 042202-042213.
13. J. Choi, Y. H. Kiem and S. H. Kye (2020), *Entangled edge states of corank one with positive partial transposes*, Journal of Mathematical Physics, Vol 61, 062202-062216.
14. C. J. Zhang, Y. S. Zhang, S. Zhang and G. C. Guo (2008), *Entanglement detecion beyond the computable cross-norm or realignment criterion*, Phys. Rev. A. Vol 77, 060301-060305.
15. Y. Guo and J. C. Hou (2013), *Realignment operation and CCNR criterion of separability for states in infinite-dimensional quantum systems*, Reports on Mathematical Physics, Vol 72, 25-40.
16. M. Horodecki, P. Horodecki and R. Horodecki (2006), *Separability of Mixed Quantum States: Linear Contractions and Permutation Criteria*, Open Syst. & Inf. Dyn. Vol 13, 103-111.
17. P. Wocjan and M. Horodecki (2005), *Characterization of Combinatorially Independent Permutation Separability Criteria*, Open Syst. & Inf. Dyn. Vol 12, 331-345.
18. L. Clarisse and P. Wocjan (2006), *On independent permutation separability criteria*, Quantum Inf. Comput. Vol 6, 277-288.
19. M. Li, Z. Wang, J. Wang, S. Shen and S. Fei (2020), *Improved lower bounds of concurrence and convex-roof extended negativity based on Bloch representations*, Quantum Inf. Process. Vol 19, 1-11.
20. H. F. Hofmann and S. Takeuchi (2003), *Violation of local uncertainty relations as a signature of entanglement*, Phys. Rev. A. Vol 68, 032103-032109.
21. O. Gühne, M. Mechler, G. Tóth and P. Adam (2006), *Entanglement criteria based on local uncertainty relations are strictly stronger than the computable cross norm criterion*, Phys. Rev. A. Vol 74, 010301-010305.
22. Y. Y. Zhao, G. Y. Xiang, X. M. Hu, B. H. Liu, C. F. Li, G. C. Guo, R. Schwonnek and R. Wolf (2019), *Entanglement Detection by Violations of Noisy Uncertainty Relations: A Proof of Principle*, Phys. Rev. Lett. Vol 122, 220401-220407.
23. C. J. Zhang, H. Nha, Y. S. Zhang and G. C. Guo (2010), *Entanglement detecion via tighter local uncertainty relations*, Phys. Rev. A. Vol 81, 012324-012329.
24. O. Gittsovich, O. Giihne, P. Hyllus and J. Eisert (2009), *Covariance matrix criterion for separability*, AIP Conference Proceedings, Vol 1110, 63-66.
25. C. J. Zhang, Y. S. Zhang, S. Zhang and G. C. Guo (2007), *Optimal entanglement witness based on local orthogonal observables*, Phys. Rew. A. Vol 76, 012334-012340.
26. K. C. Ha and S. H. Kye (2012), *Optimality for indecomposable entanglement witnesses*, Phys. Rew. A. Vol 86, 034301-034305.
27. A. Rutkowski and R. Horodecki (2014), *Tensor product extension of entanglement witnesses and their connection with measurement-device-independent entanglement witnesses*, Phys. Lett. A. Vol 378, 2043-2047.
28. S. Q. Shen, T. R. Xu, S. M. Fei and M. Li (2018), *Optimization of ultrafine entanglement witnesses*, Phys. Rew. A . Vol 97, 032343-032347.
29. R. F. Werner and M. M. Wolf(2001), *Bell inequalities and entanglement*, Quantum Information & Computation, Vol 1, 1-25.
30. C. J. Zhang, Y. S. Zhang and G. C. Guo (2007), *Genuine entanglement of generalized Bell diagonal states*, Phys. Lett. A. Vol 363, 57-56.
31. M. Li, S. M. Fei and X. Li-Jost (2011), *Bell inequality, separability and entanglement distillation*, Chinese Science Bulletin, Vol 56, 945-954.
32. H. Lee, S. D. Oh, D. Ahn (2005), *The entanglement criterion of multiqubits*, arXiv:quant-ph, 0506127-0506135.
33. S. Alheverio, S. M. Fei and D. Goswami (2001), *Separability of rank two quantum states*, Phys. Lett. A. Vol 286. 91-96.
34. S. M. Fei, X. H. Gao, X. H. Wang, Z. X. Wang and K. Wu (2002), *Separability of rank two quantum*

states on multiple quantum spaces, Phys. Lett. A. Vol 300, 559-566.

35. L. N. Gatti and J. Lacalle (2018), *A model of discrete quantum computation*, Quantum Inf. Process. Vol 17, 1-18.
36. J. Y. Zeng (2014), *Quantum Mechanics*, volume (II), 5th Edition. Science Press, Beijing.
37. M. Rosen and I. Kenneth (2013), *A Classical Introduction to Modern Number Theory*, GTM, Vol. 84. Springer Science & Business Media.

Appendix A

Property 3.1 $\mathbb{Z}[i]^{2^n}$ is a Euclidean domain.

Proof: Let $\alpha \in \mathbb{Z}[i]^{2^n}, \alpha \neq 0, \alpha = (x_0 + iy_0, \cdots, x_{2^n-1} + iy_{2^n-1})$,

$$\Phi : \alpha \longrightarrow {x_0}^2 + \cdots + {x_{2^n-1}}^2 + {y_0}^2 + \cdots + {y_{2^n-1}}^2.$$

Since $\mathbb{Z}[i]$ is a Euclidean domain, there is a mapping from the set of nonzero elements of $\mathbb{Z}[i]$ to the set of nonnegative integers, and any element b can be written in the form of $b = qa + r(q, r \in \mathbb{Z}[i])$ for a given nonzero element a in $\mathbb{Z}[i]$, here $r = 0$ or $\varphi(r) < \varphi(a)$. Easy to prove that $\varphi : a \to x^2 + y^2 (a = x + iy)$ meets the above requirements. Thus the mapping Φ can be written as $\Phi = \varphi_0 + \varphi_1 + \cdots + \varphi_{2^n-1}$, where φ_i is the above mapping corresponding to the component element α_i of α to satisfy the Euclidean domain in $\mathbb{Z}[i]$. For each φ_i, there is a pair of elements q_i, r_i, so that $\varphi_i(r_i) < \varphi_i(\alpha_i)$. Hence, for any $\beta \in \mathbb{Z}[i]^{2^n}$, there is a pair of elements $Q = (q_0, \cdots, q_{2^n-1}), R = (r_0, \cdots, r_{2^n-1})$ making $R = 0$ or $\Phi(R) < \Phi(\alpha)$. So $\mathbb{Z}[i]^{2^n}$ is a Euclidean domain □ .

Property 3.2 $\mathbb{Z}[i]^{2^n}$ is a principal ideal domain and unique factorization domain.

Proof: Because every Euclidean domain is a principal ideal domain, and thus a unique factorization domain. It can be seen from Proposition 3.1 that $\mathbb{Z}[i]^{2^n}$ is a Euclidean domain, so it is a principal ideal domain and unique factorization domain □ .

Property 3.3 There are 4^{2^n} units in $\mathbb{Z}[i]^{2^n}$.

Proof: Suppose that α is a unit, $\alpha \in \mathbb{Z}[i]^{2^n}$. Then there is an element $\beta \in \mathbb{Z}[i]^{2^n}$ that makes $\beta \cdot \alpha = I = (1, \cdots, 1)$, namely $\Phi(\alpha\beta) = \Phi(I) = 2^n$. From the definition of multiplication in $\mathbb{Z}[i]^{2^n}$, we have $\Phi(\alpha) = 2^n$ and the component of α is ± 1 or $\pm i$. Obviously, there are exactly 4^{2^n} such elements □ .

Property 3.4 Let $p_i (0 \leq i \leq 2^n - 1)$ be a prime number. The equation $x^2 + y^2 = p_i$ has no integer solution if and only if the elements in the form of $(1, \cdots, 1, p_i, 1, \cdots, 1)$ are prime elements in $\mathbb{Z}[i]^{2^n}$.

Proof: Sufficiency: Let $P = (1, \cdots, 1, p_i, 1, \cdots, 1)$. Suppose that the equation $x^2 + y^2 = p_i$ has the integer solution (x_0, y_0), then we have $p_i = (x_0 + iy_0)(x_0 - iy_0)$, where $x_0, y_0 \neq 0$. Thus P has nontrivial factors $(1, \cdots, 1, x_0 + iy_0, 1, \cdots, 1)$ and $(1, \cdots, 1, x_0 - iy_0, 1, \cdots, 1)$ This contradicts the fact that P is a prime element. So the equation $x^2 + y^2 = p_i$ has no integer solution.

Necessity: Suppose that the equation $x^2 + y^2 = p_i$ has no integer solution. We should prove P must be a prime element. If P is not a prime element, then P can be decomposed. Let $P = (1, \cdots, 1, a+ib, 1, \cdots, 1)(1, \cdots, 1, c+id, 1, \cdots, 1)$, and $a^2+b^2 \neq 1$, $c^2+d^2 \neq 1$, then $p_i = (a+ib)(c+id)$. By $\varphi(p_i) = \varphi((a+ib)(c+id))$, we have ${p_i}^2 = (a^2+b^2)(c^2+d^2)$, thus $a^2+b^2|{p_i}^2$, $c^2+d^2|{p_i}^2$. So $a^2+b^2 = {p_i}^2$ or p_i. By $c^2+d^2 \neq 1$, we get $a^2+b^2 = p_i$. And because $a, b \in \mathbb{Z}$, the equation $x^2+y^2 = p_i$ has integer solutions (a, b), which contradicts the supposition $\Box$.

Property 3.5 If the prime number $p_i (0 \leq i \leq 2^n - 1)$ can be written in the form of $4n+3$, then the elements shaped as $(1, \cdots, 1, p_i, 1, \cdots, 1)$ are prime elements in $\mathbb{Z}[i]^{2^n}$.

Proof: From Proposition 3.4, we just need to prove that the equation $4n+3 = x^2+y^2$ has no integer solution. Suppose (x_0, y_0) is the integer solution of the above equation. Let $x_0 = 2m+j, y_0 = 2n+k, m, n \in \mathbb{Z}, j, k = 0$ or 1, then $4n+3 = (2m+j)^2 + (2n+k)^2 = 4(m^2+n^2+mj+nk) + j^2+k^2$. j^2+k^2 can only be 0,1,2 , it cannot be 3. So the front formula cannot be true. Therefore, $4n+3 = x^2+y^2$ has no integer solution. This proposition is proved $\Box$.

Property 3.6 If the prime number $p_i (0 \leq i \leq 2^n - 1)$ is in the form of $4n+1$, then the elements shaped as $(1, \cdots, 1, p_i, 1, \cdots, 1)$ are nonprime elements in $\mathbb{Z}[i]^{2^n}$.

Proof: Obviously, p_i is an odd prime number. If $(1, \cdots, 1, p_i, 1, \cdots, 1)$ is not a prime element in $\mathbb{Z}[i]^{2^n}$. from Proposition 3.4, the equation $x^2+y^2 = p_i$ has an integer solution. Let the solution be (x_0, y_0). Then x_0, y_0 cannot have the same parity. Otherwise, there must be $2|p_i$. This contradicts the fact that p_i is an odd prime number. So one of x_0 and y_0 must be odd and the other even. Suppose that $x_0 = 2j, y_0 = 2k+1$, then ${x_0}^2 + {y_0}^2 = (2j)^2 + (2k+1)^2 = 4(j^2+k^2+2k)+1$. That is, ${x_0}^2+{y_0}^2$ is a prime number in the form of $4n+1$. Hence the elements shaped as $(1, \cdots, 1, p_i, 1, \cdots, 1)$ are nonprime elements in $\mathbb{Z}[i]^{2^n}$ $\Box$.

Next, we will discuss the prime elements with the from $a+bi (b \neq 0)$ in components.

Property 3.7 Let $\alpha_j = a+bi, \alpha_j \notin \mathbb{Z}, \alpha_j \in \mathbb{Z}[i], 0 \leq j \leq 2^n - 1$. a^2+b^2 is a prime number. Then the elements in the form of $(1, \cdots, 1, \alpha_j, 1, \cdots, 1)$ are prime elements in $\mathbb{Z}[i]^{2^n}$.

Proof: Let $a^2+b^2 = p$, $(1, \cdots, 1, \alpha_j, 1, \cdots, 1) = P$. Now we prove that P has only trivial factors. By the definition of multiplication in $\mathbb{Z}[i]^{2^n}$, we just need to prove α_j has no nontrivial factor in $\mathbb{Z}[i]^{2^n}$. Suppose that β is a factor for α_j, now prove that β is a trivial factor. Let $\alpha_j = \beta\gamma$, we have $\varphi(\alpha_j) = \varphi(\beta\gamma) = \varphi(\beta)\varphi(\gamma) = p$. Since p is a prime number, $\varphi(\beta) = 1$ or p. If $\varphi(\beta) = 1$, then β is a unit in $\mathbb{Z}[i]$. Also, if $\varphi(\beta) = p$, then β is an associated element. Thus P has only trivial factors. Namely the elements in the form of $(1, \cdots, 1, \alpha_j, 1, \cdots, 1)$ are prime elements in $\mathbb{Z}[i]^{2^n}$ $\Box$.

Property 3.8 Let $\alpha_j = a+bi, \alpha_j \notin \mathbb{Z}, \alpha_j \in \mathbb{Z}[i]$, $a^2+b^2 = p_1 p_2 \cdots p_n$, where $p_t (1 \leq t \leq n)$ is a prime number. We have

(i) If $n = 1$, then the element in the form of $(1, \cdots, 1, \alpha_j, 1, \cdots, 1)$ is a prime element in

$\mathbb{Z}[i]^{2^n}$.

(ii) If $n \neq 1$, then the element in the form of $(1, \cdots, 1, \alpha_j, 1, \cdots, 1)$ is a nonprime element in $\mathbb{Z}[i]^{2^n}$.

Proof: (i) From Proposition 3.7, this conclusion is established.

(ii) Obviously, $b \neq 0, a^2+b^2 = (a+bi)(a-bi) = p_1p_2\cdots p_n$. Suppose that there exists a prime number in the form of $4n+1$ or 2, and let p_2 be this prime number. By Proposition 3.6, we get $p_2 = (x_0+y_0i)(x_0-y_0i), x_0, y_0 \in \mathbb{Z}, y_0 \neq 0$, and $(a+bi)(a-bi) = p_1(x_0+y_0i)(x_0-y_0i)p_3\cdots p_n$. Since $\mathbb{Z}[i]$ is a unique factorization domain, $a+bi$ is either x_0+y_0i or it can still be factored. Because p_1 is a prime number, $a+bi$ cannot be x_0+y_0i. Thus $a+bi$ is reducible in $\mathbb{Z}[i]$. According to the definition of multiplication in $\mathbb{Z}[i]^{2^n}$, $(1, \cdots, 1, \alpha_j, 1, \cdots, 1)$ is a nonprime element. If $p_1p_2\cdots p_n$ are all prime numbers of the form $4n+3$, then $p_1p_2\cdots p_n$ is a factorization of a^2+b^2. From the property of $\mathbb{Z}[i]$, a+bi can still be factored. Hence the element in the form of $(1, \cdots, 1, \alpha_j, 1, \cdots, 1)$ is a nonprime element $\square$.

Property 3.9 If an element contains two or more components that are not 1, then the element is not a prime element in $\mathbb{Z}[i]^{2^n}$.

Proof: Let $(\alpha_0, \alpha_1, \cdots, \alpha_{2^n-1}) \in \mathbb{Z}[i]^{2^n}$, then

$$(\alpha_0, \alpha_1, \cdots, \alpha_{2^n-1}) = \prod_{j=0}^{2^n-1} (1, \cdots, 1, \alpha_j, 1, \cdots, 1)$$

If $(\alpha_0, \alpha_1, \cdots, \alpha_{2^n-1})$ contains two or more components that are not 1, Then at least two elements $(1, \cdots, 1, \alpha_j, 1, \cdots, 1)$ and $\left(1, \cdots, 1, \alpha_{j'}, 1, \cdots, 1\right)$ in the above formula are nontrivial factor of $(\alpha_0, \alpha_1, \cdots, \alpha_{2^n-1})$. Thus $(\alpha_0, \alpha_1, \cdots, \alpha_{2^n-1})$ is not a prime element in $\mathbb{Z}[i]^{2^n}$. This proposition is proved $\square$.

Property 3.10 An element in $\mathbb{Z}[i]^{2^n}$ is a prime element if and only if it is an irreducible element.

Proof: In the unique factorization domain, the element is an irreducible element if and only if it is a prime element. Because $\mathbb{Z}[i]^{2^n}$ is a unique factorization domain, the element in the ring is a prime element if and only if it is irreducible $\square$.