이학박사 학위논문

Separability of Quantum States via Algebraic Geometry

(대수 기하학을 통한 양자 상태의 분리가능성 연구)

2014년 8월

서울대학교 대학원

수리과학부

나 주 한

Separability of Quantum States via Algebraic Geometry

A dissertation
submitted in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
to the faculty of the Graduate School of
Seoul National University

by

Joohan Na

Dissertation Director : Professor Young-Hoon Kiem

Department of Mathematical Science
Seoul National University

August 2014

Abstract

Separability of Quantum States via Algebraic Geometry

Joohan Na

Department of Mathematical Sciences
The Graduate School
Seoul National University

In this thesis, we study the quantum separability problem by taking advantage of various methods in algebraic geometry.

In order to explore the separability of quantum states, we begin with the range criterion for separability. It leads us to examine the condition that $|\psi_1\rangle \otimes |\psi_2\rangle \in \mathsf{D}$ and $|\overline{\psi_1}\rangle \otimes |\psi_2\rangle \in \mathsf{E}$ for subspaces D and E of a finite-dimensional composite quantum system $\mathcal{H}_\mathsf{A} \otimes \mathcal{H}_\mathsf{B}$. More explicitly, the following two questions naturally arise : (1) For which conditions there is a nonzero product vector $|\psi_1\rangle \otimes |\psi_2\rangle$ in $\mathcal{H}_\mathsf{A} \otimes \mathcal{H}_\mathsf{B}$ such that $|\psi_1\rangle \otimes |\psi_2\rangle \in \mathsf{D}$ and $|\overline{\psi_1}\rangle \otimes |\psi_2\rangle \in \mathsf{E}$? (2) if it exists, how many such nonzero product vectors in $\mathcal{H}_\mathsf{A} \otimes \mathcal{H}_\mathsf{B}$ exist up to constant?

We investigate the question (1) and generalize it for the multipartite cases. Moreover, we answer the question (2) so that the upper bound for the number of vectors $|\psi_1\rangle \otimes |\psi_2\rangle \in \mathcal{H}_\mathsf{A} \otimes \mathcal{H}_\mathsf{B}$ satisfying the condition that $|\psi_1\rangle \otimes |\psi_2\rangle \in \mathsf{D}$ and $|\overline{\psi_1}\rangle \otimes |\psi_2\rangle \in \mathsf{E}$ is expected to be sharp for the qubit-qunit case.

Key words: entanglement, separable states, PPT states, product vectors, the range criterion, SLOCC
Student Number: 2006-20294

Contents

Chapter 1

Introduction

During the period from about 1925 until the early 1930's, physicists such as Werner Heisenberg, Erwin Schrödinger and John von Neumann established mathematical foundation of non-relativistic quantum physics [VN55]. Soon after the foundational work, however, a spooky feature of the quantum mechanics was discovered. In 1935, Albert Einstein, Boris Podolsky and Nathan Rosen wrote a paper [EPR35] challenging the very foundations of quantum mechanics. At the core of this paper lies the so-called quantum entanglement, which is a simple but counter-intuitive consequence of the mathematical formulation of quantum mechanics under the Copenhagen interpretation [Boh35].

Quantum mechanics under the Copenhagen interpretation claims that a measurement causes an instant collapse of the wave function describing the quantum system into one of the eigenstates of the observable that was measured and does not give us a measurement outcome in a deterministic way. Moreover, it asserts that a physical reality not only consists of what can be possibly observed, but also may not even exist, prior to the observation.

Einstein, Podolsky and Rosen (shortly, EPR) insisted that the theory is not complete because it violates a physical reality and the principle of locality: A physical reality means that in an experiment, the outcome of a measurement is determined before the measurement is performed, so there must exist something in the world as a real element. The principle of locality

postulates that these real elements exist locally, in the sense that spacelike separated regions are independent of one another.

These are main reasons why even prominent physicists, such as Einstein and Schrödinger, who played a key role in the history of quantum mechanics were skeptical of the quantum theory. The famous quote "God does not play dice with the universe." by Einstein and a thought experiment named "Shrödinger's cat" by Schrödinger come from their doubts on the theory.

In 1964, John Bell [Bel64] quantitatively analyzed the EPR assertion. He formalized EPR's ideas into an inequality, the so-called Bell's inequality, under the assumption of a physical reality and the principle of locality. After that, some experimental physicists [CHSH69, FC72] proposed and tried to test Bell's inequality. Eventually, it was Alain Aspect and their collegues [ADR82] that first succeeded the test of violation of Bell's inequality, so this tends to support the original formulation of quantum mechanics. It is now inevitable that the nonlocal nature of particles exists in the real world.

For a long time, the research of quantum entanglement received attention from only a few physicists who are philosophically interested in the fundamental structure of quantum physics, but the present-day entanglement theory has extensive applications such as quantum computation and algorithm [Deu85, Sho95], quantum cryptography [BB84, Eke91], quantum teleportation [BBC+93], quantum dense coding [BW92], and so on, and is now a hot research area from both angles of a fundamental theory and its applications.

1.1 Basics on quantum entanglement

In quantum mechanics, a classical example of a state is a wave function $\psi(\mathbf{r}, t) : \mathbb{R}^3 \times \mathbb{R} \longrightarrow \mathbb{C}$ at position $\mathbf{r} = (x, y, z)$ and at time t. Under the Copenhagen interpretation, the probability of a particle described by a wave function $\psi(\mathbf{r}, t)$ to appear in a region $R \subset \mathbb{R}^3$ at time t is given by

$$\int_R |\psi(\mathbf{r}, t)|^2 d\mathbf{r}.$$

Hence, the integration of $\left|\psi(\mathbf{r},t)\right|^2$ over the whole space $\mathbb{R}^3$ must be one. It is assumed that if two wave functions differ by nonzero constant, they represent the same state. Then it is reasonable to postulate the space of square integrable functions

$$L^2(\mathbb{R}^3) := \left\{ \psi(\mathbf{r},t) \;\middle|\; \int_{\mathbb{R}^3} |\psi(\mathbf{r},t)|^2 d\mathbf{r} < \infty \right\}$$

is considered as the set of all states for a fixed time t. We note that this space is a typical example of the Hilbert space which is, by definition, a complete inner product vector space over the field of complex numbers.

Keeping in mind this example, we formally define by a (pure) state an element of an abstract Hilbert space. Since we assume that two vectors represent the same state if they differ by nonzero constant, a state tends to be considered as a vector with unit norm of a Hilbert space in many physics literatures. However, due to a phase ambiguity for the definition, we sometimes consider a state as an element of the projectivization of the Hilbert space.

The simplest quantum system is $\mathbb{C}^2$ with the standard Hermitian inner product, which is the space most concerned with in Quantum computation. An element of the space $\mathbb{C}^2$ is called a quantum bit, shortly qubit. Conventionally, $\{|0\rangle, |1\rangle\}$ denotes an orthonormal basis of $\mathbb{C}^2$, so any qubit is expressed as a linear combination of $|0\rangle$ and $|1\rangle$. [1]

Now we consider a composite quantum system of the two Hilbert spaces $\mathcal{H}_A = \mathbb{C}^2$ and $\mathcal{H}_B = \mathbb{C}^2$. We suppose that a state $|\psi_1\rangle = \dfrac{|0\rangle + |1\rangle}{\sqrt{2}}$ is given

[1] $|\psi\rangle$ represents an element of a Hilbert space $\mathcal{H}$ and $\langle\psi|$ an element of the dual Hilbert space $\mathcal{H}^*$. The first one is called a ket vector, the last one a bra vector. This notation is particularly useful to denote a pairing

$$(\quad,\quad) : \mathcal{H}^* \times \mathcal{H} \longrightarrow \mathbb{C},$$

where we usually write $\langle\psi_1|\psi_2\rangle$ for the pairing $(\langle\psi_1|, |\psi_2\rangle)$, called the bra-ket notation. This is a standard notation for indicating quantum states, which was introduced by Paul Dirac.

in the first system $\mathcal{H}_A$, a state $|\psi_2\rangle = |0\rangle$ in the second system $\mathcal{H}_B$. The state $|\psi_1\rangle$ in $\mathcal{H}_A$ is the superposition of the states $|0\rangle$ and $|1\rangle$, each with the probability $\frac{1}{2}$. On the other hand, the state $|\psi_2\rangle$ in $\mathcal{H}_B$ is always $|0\rangle$ with the probability 1. Which state has to be the composite state? For simplicity, we denote by $|ab\rangle$ the composite state which is $|a\rangle$ in $\mathcal{H}_A$ and $|b\rangle$ in $\mathcal{H}_B$. Then the composite state $|\psi_1\psi_2\rangle$ is clearly the superposition of the state $|00\rangle$ and $|10\rangle$, each with the probability $\frac{1}{2}$, i.e.

$$|\psi_1\psi_2\rangle = \frac{|00\rangle + |10\rangle}{\sqrt{2}}.$$

From this observation, it is reasonable to postulate the composite quantum system is defined to be the tensor product of the two quantum systems and the composite of two given states to be the tensor product of the two states, i.e. $|\psi_1\psi_2\rangle$ is exactly $|\psi_1\rangle \otimes |\psi_2\rangle$.

More generally, the total quantum system $\mathcal{H}$ of n particles, each of which belongs to the Hilbert space $\mathcal{H}_i$ is given by the tensor product of its subsystems $\mathcal{H}_i$, i.e. $\mathcal{H} = \otimes_{i=1}^{n} \mathcal{H}_i$. Then we can write an element $|\psi\rangle$ of the total Hilbert space as follows:

$$|\psi\rangle = \sum_k |\psi_1^{(k)}\rangle \otimes |\psi_2^{(k)}\rangle \otimes \cdots \otimes |\psi_n^{(k)}\rangle,$$

where $|\psi_i^{(k)}\rangle$ are states in the individual subsystems $\mathcal{H}_i$. Note that in general, we can not describe a state $|\psi\rangle$ as a product of states of individual subsystems, i.e.

$$|\psi\rangle \neq |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle.$$

It means that when we choose a state in the total composite quantum system, it is in general not possible to assign the corresponding state in each individual subsystem. This is a radical difference between classical formalism and quantum one. According to classical mechanics, the system of total state space is the Cartesian product of their individual subsystems, so any element of the total space is always described by the corresponding state in

each individual subsystem.

This difference causes immediately a strange situation which does not occur in the classical world. For instance, let us consider the following situation: Alice and Bob are at long distance and Charles has the two particles whose state is

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{1.1}$$

in $\mathbb{C}^2 \otimes \mathbb{C}^2$. Charles sends the first particle to Alice and the second to Bob. Then if Alice obtain the state $|0\rangle$ after a measurement, then Bob's state must be the state $|0\rangle$. On the other hand, if Alice obtains $|1\rangle$ after a measurement, then Bob's state must be $|1\rangle$. This means that the results of Alice's measurement immediately affect the state of Bob's, collapsing his state no matter how long the distance is. This violates the principle of locality. We call a composite state like (1.1) an entangled state.

1.2 Quantum separability problem

Let us define entanglement more precisely. Let $\mathcal{H}$ be the composite quantum system of its subsystems $\mathcal{H}_i$, i.e. $\mathcal{H} = \otimes_{i=1}^{n} \mathcal{H}_i$. If a state $|\psi\rangle$ in $\mathcal{H}$ can be written as a tensor product of states $|\psi_i\rangle$ in the subsystems $\mathcal{H}_i$, i.e.

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle, \tag{1.2}$$

then the state $|\psi\rangle$ is called separable. Otherwise, it is called entangled. Sometimes the vector of the form (1.2) is called a product vector. The fundamental question of quantum entanglement theory is to determine whether a given state is separable or not, which is the so called quantum separability problem. We will see that the separability of this case can be easily determined in Section 3.1.

In fact, a state defined above as an element of a Hilbert space is somewhat restrictive, which is sometimes called a pure state in contrast to the notion of mixed states. A mixed state is defined by a density operator on a Hilbert space, which is a positive semi-definite Hermitian operator of trace

one on the Hilbert space. By the spectral theorem in linear algebra, a mixed state ρ on a composite quantum system $\mathcal{H} = \bigotimes_{i=1}^{n} \mathcal{H}_i$ can be expressed as

$$\rho = \sum_{k=1}^{N} p_k |\psi^{(k)}\rangle\langle\psi^{(k)}|, \tag{1.3}$$

where $\sum_{k=1}^{N} p_k = 1, p_k \geq 0$ and each $|\psi^{(k)}\rangle$ is a pure state on $\mathcal{H}$. Conversely, for any set of pairs $\{(|\psi^{(k)}\rangle, p_k)\}$ of states $|\psi^{(k)}\rangle$ with probabilities p_k, we can make a mixture of pure states of the form (1.3), which is by definition a mixed state. Note that the state vectors $|\psi^{(k)}\rangle$ in the set of pairs $\{(|\psi^{(k)}\rangle, p_k)\}$ are not necessarily orthogonal to each other.

We remark that this is a direct generalization of a pure state: For a pure state $|\psi\rangle$ in a Hilbert space $\mathcal{H}$, $\rho = |\psi\rangle\langle\psi|$ becomes a mixed state by definition. Therefore, a particular mixed state with $N = 1$ in the expression of (1.3) can be considered as a pure state. Sometimes a state of the form $|\psi\rangle\langle\psi|$ is called a product state.

Now, we define the separability of a mixed state. For the bipartite case, a mixed state ρ on a Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$ is called separable if it can be expressed as follows:

$$\rho = \sum_{k} p_k \rho_A^{(k)} \otimes \rho_B^{(k)},$$

where $\rho_A^{(k)}$ and $\rho_B^{(k)}$ are defined on the Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively [Wer89]. Note that $\rho_A^{(k)}$ and $\rho_B^{(k)}$ are assumed to be product states without loss of generality. If we write $\rho_A^{(k)} = |\psi_A^{(k)}\rangle\langle\psi_A^{(k)}|$ and $\rho_B^{(k)} = |\psi_B^{(k)}\rangle\langle\psi_B^{(k)}|$, then

$$\begin{aligned}
\rho &= \sum_{k} p_k \rho_A^{(k)} \otimes \rho_B^{(k)} \\
&= \sum_{k} p_k |\psi_A^{(k)}\rangle\langle\psi_A^{(k)}| \otimes |\psi_B^{(k)}\rangle\langle\psi_B^{(k)}| \\
&= \sum_{k} p_k |\psi_A^{(k)}\rangle \otimes |\psi_B^{(k)}\rangle\langle\psi_A^{(k)}| \otimes \langle\psi_B^{(k)}|.
\end{aligned}$$

This means that a separable mixed state is indeed a mixture of separable

product states. More generally, a state on a composite quantum system $\mathcal{H} = \bigotimes_{i=1}^{n} \mathcal{H}_i$ is said to be separable if it is a mixture of pure separable states, i.e.

$$\begin{aligned}\rho &= \sum_k p_k \rho_1^{(k)} \otimes \rho_2^{(k)} \otimes \cdots \otimes \rho_n^{(k)} \\ &= \sum_k p_k |\psi_1^{(k)}\rangle \otimes |\psi_2^{(k)}\rangle \otimes \cdots \otimes |\psi_n^{(k)}\rangle\langle\psi_1^{(k)}| \otimes \langle\psi_2^{(k)}| \otimes \cdots \otimes \langle\psi_n^{(k)}|,\end{aligned}$$

where $\sum_k p_k = 1, p_k \geq 0$ and each $\rho_i^{(k)}$ is a product state $|\psi_i^{(k)}\rangle\langle\psi_i^{(k)}|$. A state is called entangled if it is not separable.

Unlike the case of pure states, it is in general hard to determine whether a given mixed state is separable or entangled. This is known as an **NP**-hard problem [Gur03, Gha10] even for the bipartite case.

1.3 Classification of entangled states

Let us come back to a classical example for a while. Let $\psi(\mathbf{r}, t)$ be a wave function with position $\mathbf{r} = (x, y, z)$ and time t. As we mentioned above, a typical situation in quantum physics is that for a fixed time t, $\psi(\mathbf{r}, t)$ is considered as a state vector in the Hilbert space

$$L^2(\mathbb{R}^3) = \left\{ \phi(\mathbf{r}) \;\middle|\; \int_{\mathbb{R}^3} |\phi(\mathbf{r})|^2 d\mathbf{r} < \infty \right\}.$$

Now, we try to vary the time variable t. How does a state evolve? The time evolution of the state of a closed quantum system is determined by the Schrödinger equation,

$$i\hbar \frac{d\psi}{dt} = H\psi,$$

where $\hbar$ is a physical constant known as Plank's constant and H is a fixed Hermitian operator known as the Hamiltonian. This implies the Hamiltonian of a system determines the dynamics of the system completely, in principle.

For an infinitesimal time evolution Δt, the Schrödinger equation becomes

$$\psi(t+\Delta t) = \left(I - \frac{i(\Delta t)}{\hbar} H\right)\psi(t), \qquad \mod (\Delta t)^2.$$

Let $U(t_0, t)$ be a time evolution operator, i.e. $U(t_0, t)\psi(t_0) = \psi(t_0+t)$. Then we get

$$U(t, \Delta t) = I - \frac{i(\Delta t)}{\hbar} H.$$

Since H is a Hermitian operator,

$$U(t, \Delta t)\, U(t, \Delta t)^* = \left(I - \frac{i(\Delta t)}{\hbar} H\right)\left(I + \frac{i(\Delta t)}{\hbar} H\right) = I,$$

i.e. $U(t, \Delta t)$ should be a unitary operator. Since $U(t_0, t)$ is a product of infinitesimal time evolution operators, it is a unitary operator as well. By the argument above, it seems reasonable to postulate the following:

The evolution of a state in a closed quantum system is described by a unitary transformation.

Keeping in mind these observations, we define by a local unitary operation on a composite quantum system $\mathcal{H} = \otimes_{i=1}^{n} \mathcal{H}_i$ the product of local unitary groups, i.e.

$$U_1 \times U_2 \times \cdots \times U_n,$$

where each U_i is the unitary group on the Hilbert space $\mathcal{H}_i$. Its physical interpretation is the following.

Let us consider a state in a multipartite quantum system. Several parties take individual particles and are spatially separated from one another. A typical situation which we are interested in allows them to act only on their subsystems and to communicate through a classical channel. Operations of this type are called the local operations assisted by classical communications (LOCC). Since the evolution of particles is given by unitary operations in a closed system, we sometimes would like to demand that all the

local operations be unitary operations, i.e. the operation is the product of unitary groups. For these operations, the extent of entanglement is considered to be invariant.

However, the complete classification under local unitary operations is extremely hard because unitary groups are not even the algebraic groups over the complex numbers. Moreover, there are uncountably many orbits even for the bipartite qubit case [LP98]. We note that a non-invertible operation occurs only when the quantum system is not closed. For instance, time evolution is invertible whereas measurement is not. Hence, it is reasonable that we first try to classify them under the product of general linear groups, which is called the stochastic local operations assisted by the classical communications (SLOCC) in physics. This is the coarse-grained classification of entanglement and a good starting point for the classification problem [DVC00]. We deal with this problem in the last chapter.

1.4 Content of this thesis

In Chapter 2, we review some basic notions in algebraic geometry we will use. The chapter contains the notions of algebraic varieties and how to describe their properties. Several kinds of varieties which have the meaning from the quantum information point of view are introduced. Bernstein's theorem and its related results appeals the connection between the number of common roots of some given polynomials and the combinatorial object. These will be used helpfully in the later chapters.

In Chapter 3, we introduce what the quantum separability problem is, which is the main theme of this thesis. Since it is extremely hard to solve the problem in general, some necessary criteria for separability of a mixed state such as the PPT criterion and the range criterion are presented.

In Chapter 4, we give a new algebraic criterion for separability by investigating the range criterion. Building on the work [KKL11], this chapter generalize it for the multipartite cases. In particular, for the multi-qubit critical case, the algebraic criterion can be put into the permanent of the associated

matrix. In order to examine the criterion in terms of permanent, we define the equivalence of square matrices and classify all the 4×4 $(+1,-1)$-matrices with vanishing permanent, which is the first nontrivial interesting case. This chapter is based on the paper http://arxiv.org/abs/1401.3181.

In Chapter 5, we improve the results in Chapter 4 for the qubit-qunit cases by dealing with the system of equations induced from the conditions of the range criterion directly. This investigation gives us an upper bound for the number of product vectors $|\psi_1\rangle \otimes |\psi_2\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ satisfying the condition that $|\psi_1\rangle\otimes|\psi_2\rangle \in \mathsf{D}$ and $|\overline{\psi_1}\rangle\otimes|\psi_2\rangle \in \mathsf{E}$ for given subspaces D and E of $\mathcal{H}_A\otimes\mathcal{H}_B$ in terms of the mixed volume of the polynomials coming from D and E. The upper bound given here is strongly expected to be sharp by Examples in [Kye13, HK13, HK14]. This result has a noteworthy application of the length of a separable state, which is the smallest number of product vectors required to represent the separable state. This chapter is based on the paper http://arxiv.org/abs/1309.4177.

In Chapter 6, we not only distinguish the entangle states from the separable states but also classify the entangled states up to the action of invertible local operations, which is called stochastic local operations assisted by classical communication (SLOCC) in physics literatures, as further work.

Chapter 2

Classical Algebraic Geometry

Algebraic geometry is classically the field of studying algebraic varieties, which are defined by a system of polynomial equations in several variables. In particular, algebraic varieties in an affine space or a projective space and morphisms between them are the basic notions, which we mainly deal with in this chapter.

When we treat geometric objects, it is natural that we first give a suitable topology on it. In algebraic geometry, we sometimes use the so called Zariski topology, which is much coarser than the usual topology in differential or complex geometry. This is useful to define the irreducibility or dimension of an algebraic variety. Moreover, all kinds of varieties can be constructed by gluing affine varieties along open affine subsets in an affine space, just as a manifold is constructed by gluing open balls in a Euclidean space.

There are many kinds of important varieties, and we especially deal with the Segre varieties, the join and the secant varieties, the tangential varieties and the dual varieties. The dual varieties will be used to define the hyperdeterminant of a multidimensional matrix which is a generalization of the classical determinant of a square matrix. The other varieties are interesting in its own right, and they are also connected with the notions of separable states, superposition of states and their limits in quantum entanglement theory.

At the end of this chapter, we introduce Bernstein's theorem and perma-

nents. These provide us with an interesting relationship between algebraic properties and combinatorial ones. These will be mainly used in Chapter 4 and Chapter 5.

Throughout this thesis, we assume that the base field is the field $\mathbb{C}$ of complex numbers unless otherwise specified.

2.1 Affine varieties

An affine space $\mathbb{A}^n_{\mathbb{C}}$ over $\mathbb{C}$ is the set of all n-tuples of elements of $\mathbb{C}$, i.e.

$$\mathbb{A}^n_{\mathbb{C}} := \{(a_1, a_2, \cdots, a_n) \mid a_i \in \mathbb{C} \text{ for every } 1 \leq i \leq n\}.$$

This is equal to $\mathbb{C}^n$ as a set, but will be assigned a particular topological structure, called the Zariski topology. Sometimes we simply write $\mathbb{A}^n$ for $\mathbb{A}^n_{\mathbb{C}}$ if there is no confusion.

Let $\mathbb{C}[x_1, \cdots, x_n]$ be the polynomial ring in n indeterminates $x_1, \cdots, x_n$ over $\mathbb{C}$. For a polynomial $f \in \mathbb{C}[x_1, \cdots, x_n]$, we can think of f as a function from $\mathbb{A}^n$ to $\mathbb{C}$ by defining $f(P) = f(a_1, a_2, \cdots, a_n)$ for every point $P = (a_1, a_2, \cdots, a_n) \in \mathbb{A}^n$. From this standpoint, we can define the zero locus of S by

$$Z(S) := \{P \in \mathbb{A}^n \mid f(P) = 0 \text{ for all } f \in S\},$$

where S is a subset of the polynomial ring $\mathbb{C}[x_1, \cdots, x_n]$. In particular, if $S = \{f_1, f_2, \cdots, f_r\}$, we may write $Z(f_1, f_2, \cdots, f_r)$ for $Z(S)$.

Definition 2.1.1. A subset X of $\mathbb{A}^n$ is called an algebraic variety if there is a subset S of $\mathbb{F}[x_1, x_2, \cdots, x_n]$ such that $X = Z(S)$.

Let I be the ideal of $\mathbb{C}[x_1, x_2, \cdots, x_n]$ generated by S. We can readily check that $Z(S) = Z(I)$. Conversely, any ideal I in the polynomial ring $\mathbb{C}[x_1, x_2, \cdots, x_n]$ is finitely generated, i.e. there are finitely many polynomials $f_1, \cdots, f_r$ such that $I = (f_1, \cdots, f_r)$ because of the Hilbert basis theorem.

Theorem 2.1.2 (Hilbert basis theorem)**.** *[AM69, Theorem 7.5] If R is a Noetherian ring, then so is the polynomial ring $R[x]$ with coefficients in R.*

This means that when we deal with an algebraic variety, it is enough to restrict our attention to ideals in $\mathbb{C}[x_1, x_2, \cdots, x_n]$, and vice versa. For given ideals in a polynomial ring, we observe the following properties.

Proposition 2.1.3. *[Hul03, Lemma 1.1] For any collection of ideals $\{I_j\}_{j\in J}$ of $\mathbb{C}[x_1, x_2, \cdots, x_n]$, We have the following properties:*

(i) $Z(0) = \mathbb{A}^n$, $Z(\mathbb{C}[x_1, x_2, \cdots, x_n]) = \emptyset$,

(ii) $\bigcap_{j\in J} Z(I_j) = Z(\sum_{j\in J} I_j)$,

(iii) $Z(I_1) \cup Z(I_2) = Z(I_1 \cap I_2)$.

This proposition implies that algebraic varieties in an affine space $\mathbb{A}^n$ satisfy the axioms for closed sets in topology. Hence, we can define the associated topology on $\mathbb{A}^n$.

Definition 2.1.4. The Zariski topology on $\mathbb{A}^n$ is defined by taking the open sets as the complements of algebraic varieties.

Now, Z can be regarded as the map defined as follows:

$$Z \quad : \quad \left\{ \begin{array}{c} \text{ideals in} \\ \mathbb{C}[x_1, \cdots, x_n] \end{array} \right\} \quad \longrightarrow \quad \left\{ \begin{array}{c} \text{algebraic varieties} \\ \text{in } \mathbb{A}^n \end{array} \right\}$$

Naturally we may consider the reverse direction. For an algebraic variety X in $\mathbb{A}^n$, we define the ideal of X by

$$I(X) := \{f \in \mathbb{C}[x_1, x_2, \cdots, x_n] \mid f(P) = 0 \text{ for every point } P \in X\}.$$

It is not hard to see that the ideal of X is indeed an ideal. Hence I can be regarded as the map

$$I \quad : \quad \left\{ \begin{array}{c} \text{algebraic varieties} \\ \text{in } \mathbb{A}^n \end{array} \right\} \quad \longrightarrow \quad \left\{ \begin{array}{c} \text{ideals in} \\ \mathbb{C}[x_1, \cdots, x_n] \end{array} \right\}.$$

It is natural to speculate that the maps Z and I are inverses of each other. We consider the following example.

Example 2.1.5. Let a and b be complex numbers. Let $f = x - a$ and $g = y - b$ be polynomials in $\mathbb{C}[x, y]$ and an ideal $I = (f^2, g)$. Then the zero locus $Z(I)$ is the union of two lines $x = a$ and $y = b$ in the complex affine plane $\mathbb{A}^2_{\mathbb{C}}$. Now, let us consider a polynomial $h(x, y)$ which vanishes on the union of the two lines. By the division algorithm, $h(x, y)$ should be of the form $h = uf + vg$ for some polynomials u, v in $\mathbb{C}[x, y]$. This implies that $I(Z(I)) = (f, g)$. Unfortunately, this is not the same as the ideal I.

What is the problem? Intuitively, $I(Z(I))$ may bigger than I when the ideal I contains an element like f^r for an integer $r > 1$. We note that the ideal of X is, by definition, always a radical ideal, i.e. if $f^r \in I(X)$ for some positive integer r, then $f \in I(X)$.

Definition 2.1.6. For an ideal I of $\mathbb{C}[x_1, x_2, \cdots, x_n]$, the radical ideal of I is defined by

$$\sqrt{I} := \{f \in \mathbb{C}[x_1, x_2, \cdots, x_n] \mid f^r \in I \text{ for some positive integer } r\}.$$

In the discussion above, we can expect that $I(Z(I))$ may be the same as the radical ideal $\sqrt{I}$.

Theorem 2.1.7 (Hilbert's Nullstellensatz)**.** *[Mat89, Theorem 5.4] For any ideal I of $\mathbb{C}[x_1, x_2, \cdots, x_n]$,*

$$I(Z(I)) = \sqrt{I}.$$

Thus, we obtain the inverse relationship between Z and I as follows:

$$\left\{\begin{array}{c}\text{radical ideals in} \\ \mathbb{C}[x_1, \cdots, x_n]\end{array}\right\} \quad \begin{array}{c} \xrightarrow{Z} \\ \xleftarrow[I]{1:1} \end{array} \quad \left\{\begin{array}{c}\text{affine varieties} \\ \text{in } \mathbb{A}^n\end{array}\right\} \tag{2.1}$$

Now, we investigate what is the basic building blocks of algebraic varieties, such as prime numbers of integers or irreducible polynomials of polynomials.

Definition 2.1.8. A subset X of a topological space Y is said to be reducible if there are two proper closed subsets X_1 and X_2 of X such that $X_1 \cup X_2 = X$. Otherwise, X is called irreducible.

This definition seems too general at first glance, but it tells us the irreducibility of a general abstract variety, in particular, not only an affine one but also a projective one. If X is an affine variety in an affine space $\mathbb{A}^n$ with the Zariski topology, we can say whether the variety X is irreducible or not: If an affine variety X is irreducible if there are no proper algebraic subvarieties whose unions equal to X.

For an affine variety X in $\mathbb{A}^n$, $I(X)$ is the ideal in the Noetherian ring $\mathbb{C}[x_1, \cdots, x_n]$. By the definition of a Noetherian ring ([AM69, Chapter 6]), any ideal I of $\mathbb{C}[x_1, \cdots, x_n]$ has the ascending chain condition: For an ascending chain of ideals $I = I_0 \subseteq I_1 \subseteq \cdots$ of $\mathbb{C}[x_1, \cdots, x_n]$, it is stationary, i.e. there exists an integer r such that $I_r = I_{r+1} = \cdots$. We note that for algebraic varieties $X \subset Y$, their ideals have the reverse inclusion, i.e. $I(X) \supset I(Y)$, and vice versa.

Definition 2.1.9. A topological space X is said to be Noetherian if it satisfies the following condition: for any sequence of closed subsets $X_1 \supseteq X_2 \supseteq \cdots$, the sequence is stationary, i.e. there exists an integer r such that $X_i = X_r$ for every $i \geq r$. Sometimes this condition is called a descending chain condition.

By this definition, an algebraic variety X in an affine space $\mathbb{A}^n$ with the Zariski topology is Noetherian. If an affine algebraic variety X has infinitely many irreducible components X_j for $j \in J$, then we can construct a descending chain of closed subsets of X which is not stationary:

$$X = \bigcup_{j \in J} X_j \supsetneq \bigcup_{j \neq j_1} X_j \supsetneq \bigcup_{j \neq j_1, j_2} X_j \supsetneq \cdots$$

We thus have the following.

Proposition 2.1.10. *Every algebraic variety in $\mathbb{A}^n$ can be written as the finite union of irreducible affine algebraic varieties.*

By (2.1), there is an one-to-one correspondence between the affine varieties and the radical ideals. What kind of ideals correspond to irreducible affine varieties?

Suppose that an affine variety X is reducible. Then there are proper affine subvarieties Y and Z of X such that $Y \cup Z = X$. This is equivalent to $I(X) = I(Y) \cap I(Z)$, $I(X) \subsetneq I(Y)$ and $I(X) \subsetneq I(Z)$. We choose $f \in I(Y) \backslash I(X)$ and $g \in I(Z) \backslash I(X)$. Then it is clear that fg vanishes on both Y and Z, i.e. X, so $fg \in I(X)$. This observation leads to the following proposition.

Proposition 2.1.11. *[Hul03, Proposition 1.8] Let X be a nonempty affine variety in $\mathbb{A}^n$. Then the variety X is irreducible if and only if its ideal $I(X)$ is a prime ideal.*

For a point $(a_1, a_2, \cdots, a_n) \in \mathbb{A}^n$, we can consider the point as an affine variety $\bigcap_{i=1}^{n} Z(x_i - a_i) = Z((x_1 - a_1, x_2 - a_2, \cdots, x_n - a_n))$ by Proposition 2.1.3. Note that $I(X) = (x_1 - a_1, x_2 - a_2, \cdots, x_n - a_n)$ and it is a maximal ideal of $\mathbb{C}[x_1, \cdots, x_n]$. Thus every maximal ideal of the polynomial ring $\mathbb{C}[x_1, \cdots, x_n]$ is of the form $(x_1 - a_1, x_2 - a_2, \cdots, x_n - a_n)$ for a point $(a_1, a_2, \cdots, a_n) \in \mathbb{A}^n$ by the Hilbert's Nullstellensatz. To summarize what we have discussed, we get the following:

$$\begin{array}{ccc}
\left\{ \begin{array}{c} \text{affine varieities} \\ \text{in } \mathbb{A}^n \end{array} \right\} & \underset{Z}{\overset{I}{\rightleftarrows}} & \left\{ \begin{array}{c} \text{radical ideals in} \\ \mathbb{C}[x_1, \cdots, x_n] \end{array} \right\} \\
\bigcup & & \bigcup \\
\left\{ \begin{array}{c} \text{irreducible affine varieities} \\ \text{in } \mathbb{A}^n \end{array} \right\} & \underset{Z}{\overset{I}{\rightleftarrows}} & \left\{ \begin{array}{c} \text{prime ideals in} \\ \mathbb{C}[x_1, \cdots, x_n] \end{array} \right\} \\
\bigcup & & \bigcup \\
\{ \text{ points in } \mathbb{A}^n \} & \underset{Z}{\overset{I}{\rightleftarrows}} & \left\{ \begin{array}{c} \text{maximal ideals in} \\ \mathbb{C}[x_1, \cdots, x_n] \end{array} \right\}
\end{array}$$

We remark that the correspondence above holds for the base field to be algebraically closed field. For instance, the ideal $(x^2 + 1)$ of $\mathbb{R}[x]$ is an maximal ideal, but $Z(x^2 + 1)$ is empty.

Let X be an affine variety. So far, we have considered the ideal of X as an algebraic object corresponding to the given geometric object X, but now we consider the quotient ring $\mathbb{C}[x_1, \cdots, x_n]/I(X)$ instead of the ideal $I(X)$. We will see that this viewpoint has advantages to deal with varieties together with morphisms between them.

Definition 2.1.12. For an affine variety $X \subset \mathbb{A}^n$, A map $f : X \longrightarrow \mathbb{C}$ is called a polynomial function on X if there is a polynomial $F \in \mathbb{C}[x_1, \cdots, x_n]$ such that $f(P) = F(P)$ for all $P \in X$.

Let F and G be two polynomials in $\mathbb{C}[x_1, \cdots, x_n]$. The restrictions of F and G to X determine the polynomial functions f and g on X respectively. We note that the two polynomial functions f and g on X are the same, i.e. $f(P) = g(P)$ for every point $P \in X$ whenever the restriction of the polynomial $F-G$ to X is identically zero as a function. This is equivalent to the condition that the polynomial $F - G$ belongs to the ideal $I(X)$. This observation leads to the following definition.

Definition 2.1.13. For an affine variety X in $\mathbb{A}^n$, $I(X)$ denotes the ideal of X. We define by the affine coordinate ring of X

$$A(X) := \mathbb{C}[x_1, x_2, \cdots, x_n]/I(X).$$

Note that the affine coordinate ring $A(X)$ is the set of polynomial functions on X as well as indeed the ring under the usual addition and product of functions. In fact, it is a finitely generated reduced $\mathbb{C}$-algebra, i.e. a finitely generated $\mathbb{C}$-algebra with no nilpotent elements because $I(X)$ is a radical ideal. We remark that if X is irreducible, then $I(X)$ is a prime ideal of $\mathbb{C}[x_1, \cdots, x_n]$, so $A(X)$ is an integral domain.

Let $X \subset \mathbb{A}^m$ and $Y \subset \mathbb{A}^n$ be affine varieties. A map $f : X \longrightarrow Y$ is said to be a morphism if there are polynomial functions $f_1, f_2, \cdots, f_n$ on X such that

$$\begin{array}{ccccc} f & : & X & \longrightarrow & Y \\ & & \mathbf{x} = [x_1 : \cdots : x_m] & \mapsto & [f_1(\mathbf{x}) : \cdots : f_n(\mathbf{x})] \end{array}$$

A morphism is an isomorphism if it has an inverse morphism. For a morphism $f : X \longrightarrow Y$ and a polynomial function $\varphi \in A(Y)$, their composition

$\varphi \circ f$ a polynomial function on X, so this induces a $\mathbb{C}$-algebra homomorphism

$$\begin{array}{ccccc} f^* & : & A(Y) & \longrightarrow & A(X) \\ & & \varphi & \mapsto & \varphi \circ f \end{array}$$

Therefore, we can easily check that this defines the equivalence of categories between the category of affine varieties over $\mathbb{C}$ and the category of finitely generated reduced $\mathbb{C}$-algebras.

$$\begin{array}{ccc} \{ \text{ affine varieties over } \mathbb{C} \} & \xrightarrow{\sim} & \{ \text{ finitely generated reduced } \mathbb{C}\text{-algebras } \} \\ X & \mapsto & A(X) \\ X \xrightarrow{f} Y & \mapsto & A(Y) \xrightarrow{f^*} A(X) \end{array}$$

2.2 Projective varieties

Let L_1 and L_2 be lines in the real affine plane $\mathbb{R}^2$. These two lines meet a single point in general. However, they may not intersect, i.e. they are parallel. In order to remove the case where two lines are parallel, we add points at infinity to the real affine plane $\mathbb{R}^2$ so that any two parallel lines meet a point at infinity. We call this new plane the projective real plane $\mathbb{RP}^2$. Keeping in mind this example, we define the projective space as follows.

Definition 2.2.1. For a given finite dimensional complex vector space V, we define by the projective space

$$\mathbb{P}V := V - \{0\}/\sim,$$

where two vectors $\mathbf{v}$ and $\mathbf{w}$ in V are equivalent, i.e. $\mathbf{v} \sim \mathbf{w}$, if and only if $\mathbf{v} = c\mathbf{w}$ for some $c \in \mathbb{C}^*$.

Of course, we can define a projective space over any base field $\mathbb{F}$, such as $\mathbb{R}$, in the same way, but we focus only on the case defined over $\mathbb{C}$ in this thesis.

When we fix a basis for the vector space V so that $V \cong \mathbb{C}^{n+1}$, we can write a point $p = [x_0 : x_1 : \cdots : x_n]$ in $\mathbb{P}V$ in terms of coordinates, which is so called homogeneous coordinates. In this case, we may write $\mathbb{P}^n$ for $\mathbb{P}(\mathbb{C}^{n+1})$. Sometimes we write $\mathbb{CP}^n$ instead of $\mathbb{P}^n$ for emphasizing its base field.

By the definition of the projective space $\mathbb{P}^n$, we note that not all the coordinates x_i should be zero and if two vectors $(x_0, \cdots, x_n)$ and $(x_0, \cdots, x_n)$ in $\mathbb{C}^{n+1}$ differ by nonzero constant multiples, they correspond to the same point $[x_0 : x_1 : \cdots : x_n] = [y_0 : y_1 : \cdots : y_n]$ in $\mathbb{P}^n$.

Let us consider the subset $U_0 := \{[x_0 : \cdots : x_n] \in \mathbb{P}^n \mid x_0 \neq 0\}$. There is an isomorphism between $\mathbb{A}^n$ and U_0

$$\begin{array}{ccccc} \mathbb{A}^n & & \xrightarrow{\sim} & & U_0 \quad \subset \quad \mathbb{P}^n \\ (x_1, \cdots, x_n) & & \mapsto & & [1 : x_1 : \cdots, x_n] \\ \left(\dfrac{x_1}{x_0}, \cdots, \dfrac{x_n}{x_0}\right) & & \mapsfrom & & [x_0 : x_1 : \cdots, x_n] \end{array}$$

In this case, a point $[0 : x_1 : \cdots : x_n]$ is called a point at infinity, which meets the lines parallel to the line passing through $[1 : 0 : \cdots : 0]$ and $[1 : x_1 : \cdots : x_n]$. Hence, the locus $\{x_0 = 0\}$ in $\mathbb{P}^n$ can be considered as the set of points at infinity. Since at least one of the coordinates is not zero, all the $U_i := \{[x_0 : \cdots : x_n] \in \mathbb{P}^n \mid x_i \neq 0\}$'s cover the projective space $\mathbb{P}^n$, i.e.

$$\mathbb{P}^n = U_0 \cup U_1 \cup \cdots \cup U_n.$$

These U_i are called the affine charts of $\mathbb{P}^n$, which are Zariski open subsets of $\mathbb{P}^n$ as we will give the Zariski topology on it.

In order to say the notion of varieties in a projective space as in an affine space, we introduce some algebraic notions. A ring R is called a graded ring if there is a decomposition $R = \bigoplus_{d=0}^{\infty} R_d$ of abelian groups such that $R_d \cdot R_e \subseteq R_{d+e}$ for every d, e. An element f of the graded ring R is called homogeneous of degree d if it belongs to R_d. An ideal of a graded ring R is a homogeneous ideal if it can be generated by homogeneous elements of R, i.e. $I = \bigoplus_{d=0}^{\infty}(I \cap R_d)$.

The typical example of a graded ring is the polynomial ring $\mathbb{C}[x_0, \cdots, x_n]$.

If we denote by $\mathbb{C}[x_0, \cdots, x_n]_d$ the vector space of degree d polynomials of $\mathbb{C}[x_0, \cdots, x_n]$, then the ring $\mathbb{C}[x_0, \cdots, x_n]$ has a natural graded structure.

Let $f(x_0, \cdots, x_n)$ be a homogeneous polynomial of degree d over $\mathbb{C}$. Then f satisfies

$$f(\lambda x_0, \lambda x_1, \cdots, \lambda x_n) = \lambda^d \cdot f(x_0, x_1, \cdots, x_n)$$

for every $\lambda \in \mathbb{C}^*$. This implies that a homogeneous polynomial f of positive degree can not be a function on $\mathbb{P}^n$. For example, although the two points $(1, 2)$ and $(2, 4)$ in $\mathbb{C}^2$ represent the same point in $\mathbb{P}^1$, $f(1, 2) \neq f(2, 4)$ for $f(x, y) = x^2 + xy$. However, it does make sense to say the zero locus of the polynomial f since $f(x_0, x_1, \cdots, x_n) = 0$ is independent of the choice of a representative of $[x_0 : x_1 : \cdots : x_n]$.

Definition 2.2.2. Let S be a subset of homogeneous polynomials of the polynomial ring $\mathbb{C}[x_0, \cdots, x_n]$. We define by the zero locus of S

$$Z(S) := \{P \in \mathbb{P}^n \mid f(P) = 0 \text{ for all } f \in S\}.$$

In particular, if $S = \{f_1, f_2, \cdots, f_r\}$, we may write $Z(f_1, f_2, \cdots, f_r)$ for $Z(S)$.

A subset X of $\mathbb{P}^n$ is called a projective variety if $X = Z(S)$ for a set of homogeneous polynomials S of $\mathbb{C}[x_0, \cdots, x_n]$. As for the affine case, $Z(I) = Z(S)$ for the homogeneous ideal I generated by S. Moreover, since any homogeneous ideal is finitely generated, $I = (f_1, f_2, \cdots, f_r)$ for some homogeneous polynomials $f_1, f_2, \cdots, f_r$ of $\mathbb{C}[x_0, \cdots, x_n]$. The following proposition shows that the set of all projective varieties of a projective space give rise to a topology on the projective space.

Proposition 2.2.3. *[Har77, Proposition 2.1] The empty set and the whole projective space are projective varieties, the finite union of projective varieties is a projective variety and the intersection of (possibly infinitely many) projective varieties is a projective variety.*

We define the Zariski topology on $\mathbb{P}^n$ by taking the open subsets as the complements of projective varieties. For a projective variety X of $\mathbb{P}^n$, we define by the homogeneous ideal $I(X)$ of X the ideal generated by the homogeneous polynomials f of $\mathbb{C}[x_0, \cdots, x_n]$ such that $f(P) = 0$ for every point

$P \in X$. The question whether there is an one-to-one correspondence between projective varieties and homogeneous ideals naturally arises as for the affine case.

For a homogeneous ideal I of $\mathbb{C}[x_0, \cdots, x_n]$, we consider the zero set of I in the affine space $\mathbb{A}^{n+1}$, not in the projective space $\mathbb{P}^n$, which we denote by $\widehat{Z}(I)$. If we consider the natural projection map

$$\pi : \mathbb{A}^{n+1} \backslash \{0\} \longrightarrow \mathbb{P}^n, \tag{2.2}$$

$\widehat{Z}(I)$ is nothing but $\widehat{Z}(I) = \pi^{-1}(Z(I)) \cup \{0\}$. We note that if $(a_0, \cdots, a_n)$ is an element of $\widehat{Z}(I)$, then so are all the points $(\lambda a_0, \cdots, \lambda a_n)$ for $\lambda \in \mathbb{C}^*$.

Definition 2.2.4. For a homogeneous ideal I of $\mathbb{C}[x_0, \cdots, x_n]$, the affine variety $\widehat{Z}(I)$ is called the affine cone over the projective variety $Z(I)$ in $\mathbb{P}^n$.

Suppose $Z(I) = \emptyset$ for a homogeneous ideal I of $\mathbb{C}[x_0, \cdots, x_n]$. This implies the condition $\widehat{Z}(I) \subseteq \{0\}$ by definition. By the Hilbert's Nullstellensatz, this is equivalent to the condition $\sqrt{I} \supseteq I(\{0\}) = (x_0, \cdots, x_n)$. Since the ideal $(x_0, \cdots, x_n)$ is a maximal ideal, the possibilities are either $\sqrt{I} = (x_0, \cdots, x_n)$ or $\sqrt{I} = \mathbb{C}[x_0, \cdots, x_n]$. We notice that $I(\emptyset) = \mathbb{C}[x_0, \cdots, x_n]$. The projective version of the Hilbert's Nullstellensatz says that the analogue of of Theorem 2.1.7 holds if we just exclude the exceptional case.

Theorem 2.2.5. *For a homogeneous ideal* I *of* $\mathbb{C}[x_0, \cdots, x_n]$,

$$I(Z(I)) = \sqrt{I}$$

whenever its radical ideal $\sqrt{I}$ *is not the ideal* $\mathfrak{m} := (x_0, \cdots, x_n)$*, so called the irrelevant ideal.*

Thus, we obtain the following as for the affine case:

$$\left\{ \begin{array}{c} \text{homogeneous radical ideals} \\ I \neq \mathfrak{m} \text{ in } \mathbb{C}[x_0, \cdots, x_n] \end{array} \right\} \underset{I}{\overset{Z}{\underset{\longleftarrow}{\overset{\longrightarrow}{1:1}}}} \left\{ \begin{array}{c} \text{projective varieties} \\ X \text{ in } \mathbb{P}^n \end{array} \right\} \tag{2.3}$$

We note that a projective variety X of $\mathbb{P}^n$ with the Zariski topology is a Noetherian topological space as for the affine case. By definition 2.1.8, a

projective variety $X \subset \mathbb{P}^n$ is said to be reducible if there are proper projective varieties Y and Z other than X such that $Y \cup Z = X$. Otherwise, X is called irreducible. In the same way of the affine case, we can obtain the following.

$$\begin{array}{ccc}
\left\{ \begin{array}{c} \text{projective varieities} \\ X \text{ in } \mathbb{P}^n \end{array} \right\} & \begin{array}{c} \xrightarrow{I} \\ \xleftarrow[Z]{} \end{array} & \left\{ \begin{array}{c} \text{homogeneous radical ideals} \\ I \neq \mathfrak{m} \text{ in } \mathbb{C}[x_0, \cdots, x_n] \end{array} \right\} \\
\bigcup & & \bigcup \\
\left\{ \begin{array}{c} \text{irreducible projective} \\ \text{varieities } X \text{ in } \mathbb{P}^n \end{array} \right\} & \begin{array}{c} \xrightarrow{I} \\ \xleftarrow[Z]{} \end{array} & \left\{ \begin{array}{c} \text{homogeneous prime ideals} \\ I \neq \mathfrak{m} \text{ in } \mathbb{C}[x_0, \cdots, x_n] \end{array} \right\} \\
\bigcup & & \bigcup \\
\{ \text{ points } P \text{ in } \mathbb{P}^n \ \} & \begin{array}{c} \xrightarrow{I} \\ \xleftarrow[Z]{} \end{array} & \left\{ \begin{array}{c} \text{homogeneous maximal ideals} \\ I \neq \mathfrak{m} \text{ in } \mathbb{C}[x_0, \cdots, x_n] \end{array} \right\}
\end{array}$$

As for the affine case, we can consider the analogue of the affine coordinate ring for the projective case.

Definition 2.2.6. Let X be a projective variety in $\mathbb{P}^n$ and $I(X)$ the homogeneous ideal of X. The homogeneous coordinate ring of X is defined by

$$S(X) := \mathbb{C}[x_0, \cdots, x_n]/I(X).$$

We can readily check that the homogeneous coordinate ring $S(X)$ is indeed a graded ring, i.e.

$$S(X) = \bigoplus_{d=0}^{\infty} S(X)_d$$

because $I(X)$ is a homogeneous ideal. Unlike the affine case, we remark that an element of a homogeneous coordinate ring $S(X)$ is not a polynomial function on X. However, $S(X)$ contains all information of regular functions on every open subset U of X in the following sense: Let f and g be both homogeneous elements of the same degree d in $S(X)$. Although they can not be polynomial functions on X, the quotient $\dfrac{f}{g}$ is well defined on the complement

of the zero locus $Z(g)$, i.e.

$$\frac{f(\lambda \mathbf{x})}{g(\lambda \mathbf{x})} = \frac{\lambda^d f(\mathbf{x})}{\lambda^d g(\mathbf{x})} = \frac{f(\mathbf{x})}{g(\mathbf{x})}$$

for every point $\mathbf{x} \in \widehat{X}$ and $\lambda \in \mathbb{C}^*$ whenever g is not an element in the ideal $I(X)$. A function of this type is called a rational function on X.

Definition 2.2.7. The function field of X is defined by the field of rational functions on X, i.e.

$$K(X) := \left\{ \frac{f}{g} \;\middle|\; f, g \in S(X)_d \text{ for some integer } d,\ g \notin I(X) \right\}$$

A rational function h on X is called regular at a point $P \in X$ if there are elements f and g in $S(X)_d$ such that $h = \frac{f}{g}$ and $g(P) \neq 0$. Let X be a projective variety in $\mathbb{P}^n$ and $U_f = X \backslash Z(f)$ an basic open subset of X for a homogeneous polynomial f of degree d in $\mathbb{C}[x_0, \cdots, x_n]$ which does not vanish identically on X. Then the set of all regular functions on U_f is exactly

$$S(X)_{(f)} = \left\{ \frac{g}{f^n} \;\middle|\; g \in S(X)_{dn} \right\},$$

and which gives us what is the set of regular functions on any affine open subset of X [Har77, Chapter I, Theorem 3.4]. In fact, the set of regular functions on an affine variety is exactly the set of polynomial functions on X [Har77, Chapter I, Theorem 3.2]. Hence, a morphism between affine varieties can be considered a map given by tuples of regular functions. However, this definition is not available on the projective case because the possible regular function on the whole projective variety X is only a constant function. So, we have to define the morphism between projective varieties locally.

Definition 2.2.8. Let $X \subset \mathbb{P}^n$ and $Y \subset \mathbb{P}^m$ be projective varieties. A map $\phi : X \longrightarrow Y$ is said to be a morphism of projective varieties if for any $p \in X$, there exists a Zariski open neighborhood $p \in U \subseteq X$ such that there

are homogeneous polynomials $f_0, f_1, \cdots, f_m$ in $\mathbb{C}[x_0, x_1, \cdots, x_n]$ of the same degree such that the restriction $\phi|_U$ can be written as

$$\begin{array}{ccccc} \phi|_U & : & U & \longrightarrow & Y \\ & & \mathbf{x} = [x_0 : \cdots : x_n] & \mapsto & [f_0(\mathbf{x}) : f_1(\mathbf{x}) : \cdots : f_m(\mathbf{x})] \end{array}$$

An isomorphism of projective varieties is a morphism with an inverse morphism. Practically, the morphism of projective varieties is often given by globally defined homogeneous polynomials, but it does not always.

Example 2.2.9. Let X be the zero locus of $xz - y^2$ in $\mathbb{P}^2$. We define a morphism $\phi : X \longrightarrow \mathbb{P}^1$ by

$$\phi([x : y : z]) = \begin{cases} [x : y] & \text{if } x \neq 0 \\ [y : z] & \text{if } z \neq 0 \end{cases}$$

If $x = z = 0$, then $y = 0$ as well, so this does not happen. It implies that ϕ is well-defined. Note that there are no pair of homogeneous polynomials (f_0, f_1) on $\mathbb{P}^2$ for which $[f_0 : f_1]$ agrees with ϕ.

2.3 Dimension and degree

Let us consider the projective plane $\mathbb{P}^2$. There is no doubt that we would say the dimension of $\mathbb{P}^2$ is 2. How to justify it rigorously? The idea to define the dimension in algebraic geometry is the following: if X is an irreducible variety, then any closed subvarieties of X other than X must have dimension at least one smaller.

Definition 2.3.1. Let X be an irreducible Noetherian topological space. The dimension of X is the maximum number n such that there is a chain

$$\emptyset \subsetneq X_0 \subsetneq X_1 \subsetneq \cdots \subsetneq X_n = X$$

of irreducible closed subsets of X. If X is any Noetherian topological space,

the dimension of X is defined to be the supremum of the dimensions of its irreducible components.

As for the definition of irreducibility, the definition 2.3.1 gives us what the dimension of an affine or a projective variety with the Zariski topology: the dimension of a variety X is the largest number n such that there is a chain $\emptyset \subsetneq X_0 \subsetneq X_1 \subsetneq \cdots \subsetneq X_n = X$ of irreducible closed subvarieties of X.

An 1-dimensional variety is sometimes called a line and a 2-dimensional a surface. An hypersurface in $\mathbb{A}^n$ or $\mathbb{P}^n$ is a variety of dimenion $n-1$. In particular, a hypersurface of degree one is called a hyperplane.

Although the definition 2.3.1 is plausible intuitively, it is not practical to calculate the dimension of a given variety. For a projective variety X in $\mathbb{P}^n$, we introduce a polynomial given by X, so called the Hilbert polynomial, which has much geometric information of the variety X such as the dimension and the degree of X.

Definition 2.3.2. Let $X \subset \mathbb{P}^n$ be a projective variety and $S(X)$ the homogeneous coordinate ring of X. The Hilbert function is defined by

$$H_X(m) := \dim S(X)_d,$$

where $S(X)_d$ is the vector space of the degree d part of the homogeneous coordinate ring $S(X)$.

Proposition 2.3.3. *[Har92, Proposition 13.2] If we ignore some small values of m, the Hilbert function $H_X(m)$ agrees with a polynomial in $\mathbb{Z}[m]$, denoted by $h_X(m)$. Moreover, the degree of the Hilbert polynomial of X is equal to the dimension of X.*

The polynomial $h_X(m)$ is called the Hilbert polynomial of X. Now, we give some examples in order to elucidate which information is induced from the polynomial.

Let X be a projective variety in $X = \mathbb{P}^n$. Let $H = Z(L)$ be a hyperplane given by a linear polynomial L in which there are no irreducible components

of X. Let us consider the following exact sequence:

$$0 \to S/I(X) \to S/I(X) \to S/\left((L) + I(X)\right) \to 0,$$

where $S = \mathbb{C}[x_0, \cdots, x_n]$ and the first nontrivial map is the multiplication by L. It is easily checked that the first nontrivial map is injective because no irreducible components of X are contained in H. For sufficiently large m, we can obtain the sequence of vector spaces

$$0 \to \left(S/I(X)\right)_{m-1} \to \left(S/I(X)\right)_m \to \left(S/\left((L) + I(X)\right)\right)_m \to 0.$$

If we calculate the degree of each terms of the exact sequence above, we get

$$h_{X\cap H}(m) = h_X(m) - h_X(m-1). \tag{2.4}$$

We observe the following:

- If the degree of the polynomial $h_X(m)$ is d, then the degree of $h_{X\cap H}(m)$ is $d-1$.
- Since $h_{\mathbb{P}^0}(m) = \dim \mathbb{C}[x]_m = 1$ for every m, the degree of the Hilbert polynomial of a point is 0.

From these observations, the following theorem is reasonable.

Theorem 2.3.4. *[Har92, Proposition 13.2] Let X be a projective variety in $\mathbb{P}^n$. Then the degree of the Hilbert polynomial h_X is the dimension of X.*

Now, let us think how to define the degree of an r-dimensional projective variety X in $\mathbb{P}^n$. Intuitively, the degree of X is given by the number of intersection points of X and r general hyperplanes.

Example 2.3.5. Let X be the set of distinct d points $p_1, p_2, \cdots, p_d$ in $\mathbb{P}^n$. We consider the following linear map.

$$\begin{array}{ccccc} \phi & : & \mathbb{C}[x_0, \cdots, x_n]_m & \longrightarrow & \mathbb{C}^d \\ & & f & \mapsto & (f(p_1), f(p_2), \cdots, f(p_d)) \end{array}$$

Note that the kernel of ϕ is exactly $I(X)_m$. If we show that ϕ is surjective for sufficiently large m, then the dimension of $(\mathbb{C}[x_0, \cdots, x_n]/I(X))_m$ becomes d, i.e. $h_X(m) = d$. Let L_i be a linear polynomial vanishing at p_i, but not p_j for every $j \neq i$. Let f_j be the polynomial $\prod_{i \neq j} L_i$ of degree $d-1$. Then f_j vanishes all the points p_i for $i \neq j$, except p_j. This means that when $m = d-1$, each point of $\mathbb{C}^d$ belongs to the image of a linear combination of f_j's, i.e. ϕ is surjective. When $m > d-1$, the same situation works if we multiply f_j by some L_i's for $i \neq j$. Therefore, the Hilbert function $H_X(m) = d$ for $m \geq d-1$, so the Hilbert polynomial h_X is d.

In order to investigate the higher dimensional case, we write the Hilbert polynomial $h_X(m)$ as follows:

$$h_X(m) = \frac{a_r}{r!}m^r + \frac{a_{r-1}}{(r-1)!}m^{r-1} + O(m^{r-2}).$$

By the equation (2.4),

$$h_{X \cap H}(m) = \frac{a_r}{(r-1)!}m^{r-1} + O(m^{r-2}).$$

Hence we observe the following.

- For a general hyperplane H in $\mathbb{P}^n$, h_X and $h_{X \cap H}$ have the same number a_r which is the product of the leading coefficient of the Hilbert polynomial and the factorial of the degree of the Hilbert polynomial.
- When X is a variety of distinct d points, $h_X(m)$ is a constant number d by the example 2.3.5.

Keeping in mind these observations, we define the degree of X as follows.

Definition 2.3.6. Let X be an r-dimensional projective variety in $\mathbb{P}^n$. Then the degree of X is defined by $r!$ times the leading coefficient of the Hilbert polynomial $h_X(m)$, i.e.

$$\deg X := r! \cdot a_r,$$

where the Hilbert polynomial $h_X(m) = a_r m^r + a_{r-1}m^{r-1} + \cdots + a_0$.

Example 2.3.7. For a homogeneous polynomial f of degree d in $\mathbb{C}[x_0, \cdots, x_n]$, let X be the hypersurface $Z(f)$ in $\mathbb{P}^n$. Then its homogeneous coordinate ring $S(X)$ is the ring $\mathbb{C}[x_0, \cdots, x_n]/(f)$. Let us consider the following exact sequence.

$$0 \to \mathbb{C}[x_0, \cdots, x_n] \to \mathbb{C}[x_0, \cdots, x_n] \to \mathbb{C}[x_0, \cdots, x_n]/(f) \to 0,$$

where the first nontrivial map is the multiplication by f. For an integer m with $m > d$, we get the following.

$$\begin{aligned} h_X(m) &= h_{\mathbb{P}^n}(m) - h_{\mathbb{P}^n}(m-d) \\ &= \binom{n+m}{n} - \binom{n+m-d}{n} \\ &= \frac{d}{(n-1)!} m^{n-1} + O(m^{n-2}) \end{aligned}$$

Hence, the hypersurface has the dimension $n-1$ and the degree d.

Theorem 2.3.8 (Bezout's theorem)**.** *Let f and g be homogeneous polynomials of degree d and e in $\mathbb{C}[x_0, x_1, x_2]$ respectively. Let $C = Z(f)$ and $D = Z(g)$ be the two curves defined by f and g in the projective plane $\mathbb{P}^2$. If the curves C and D have no common irreducible components, then the number of intersection points of C and D is de counting with multiplicities.*

Proof. Let us consider the following exact sequence:

$$0 \to \mathbb{C}[x_0, x_1, x_2]/(f) \to \mathbb{C}[x_0, x_1, x_2]/(f) \to \mathbb{C}[x_0, x_1, x_2]/(f, g) \to 0, \quad (2.5)$$

where the first nontrivial map is given by multiplication by g. Since f and g have no common factors, the first nontrivial map is injective. We note that the Hilbert polynomial of the curve C is $h_C(m) = dm + \alpha$ for some $\alpha \in \mathbb{Z}$

by Example 2.3.7. From the sequence (2.5), we obtain the following.

$$\begin{aligned} h_{C\cap D}(m) &= h_C(m) - h_C(m-e) \\ &= (dm+\alpha) - (d(m-e)+\alpha) \\ &= de. \end{aligned}$$

Hence, $C\cap D$ is zero-dimensional and the number of points in $C\cap D$ counting with multiplicities is exactly de. □

Before closing this section, we introduce another method to calculate the degree of a variety or the number of points of the intersection of varieties. It is based on algebraic topology and differential topology, so we assume the base field is not the field of complex numbers $\mathbb{C}$, but the field of real numbers $\mathbb{R}$. See [Hat02, GH11] for more details.

Let X be a closed oriented smooth manifold of real dimension n. Let Y and Z be oriented smooth submanifolds of dimension $n-k$ and $n-\ell$ respectively. Assume that they intersect transversely, i.e. for every point P in $Y\cap Z$, the map of tangent spaces $T_PY\oplus T_PZ \longrightarrow T_PX$ induced by the inclusions $T_PY \hookrightarrow T_PX$ and $T_PZ \hookrightarrow T_PX$ is surjective. Then $Y\cap Z$ is a submanifold of dimension $n-k-\ell$ and the following exact sequence satisfies:

$$0 \to T_P(Y\cap Z) \to T_PY \oplus T_PZ \to T_PX \to 0.$$

We note that this sequence determines an orientation of $Y\cap Z$: We take $v_1, v_2, \cdots, v_{n-k-\ell}$ as the oriented basis for the tangent space $T_p(Y\cap Z)$ satisfies the following.

(i) there exist $u_1, u_2, \cdots, u_k$ in T_pY such that $u_1, \cdots, u_k, v_1, \cdots, v_{n-k-\ell}$ is a basis for T_pY.

(ii) there exist $w_1, w_2, \cdots, w_\ell$ in T_pZ such that $v_1, \cdots, v_{n-k-\ell}, w_1, \cdots, w_\ell$ is a basis for T_pZ.

(iii) the basis $u_1, \cdots, u_k, v_1, \cdots, v_{n-k-\ell}, w_1, \cdots, w_\ell$ for T_pX is positively oriented.

Then we can give the orientation $\nu_1, \nu_2, \cdots, \nu_{n-k-\ell}$ to the intersection $Y \cap Z$. The intersection $Y \cap Z$ with the orientation is called the intersection cycle of Y and Z of dimension $n-k-\ell$.

For given two submanifolds Y and Z of X defined as above, let us consider the corresponding homology classes $[Y] \in H_{n-k}(X, \mathbb{Z})$ and $[Z] \in H_{n-\ell}(X, \mathbb{Z})$. Their intersection cycle defines a homology class $[Y \cap Z] \in H_{n-k-\ell}(X, \mathbb{Z})$. By the Poincaré duality theorem, the three classes can be considered as the cohomology classes $[Y] \in H^k(X, \mathbb{Z})$, $[Z] \in H^\ell(X, \mathbb{Z})$ and $[Y \cap Z] \in H^{k+\ell}(X, \mathbb{Z})$. Moreover, It is well known that cup product of two cohomology classes is Poincare dual to intersection of two corresponding cycles by the Poincaré duality, i.e.

$$[Y] \cup [Z] = [Y \cap Z] \in H^{k+\ell}(X, \mathbb{Z}). \tag{2.6}$$

If we define the multiplication on $\bigoplus_{i \geq 0} H^i(X, \mathbb{Z})$ as cup product, then $H^*(X, \mathbb{Z}) := \bigoplus_{i \geq 0} H^i(X, \mathbb{Z})$ with the multiplication has a natural graded ring structure, so it is called the cohomology ring of X. For two classes α and β in $H^*(X, \mathbb{Z})$, we may write $\alpha \cdot \beta$ for $\alpha \cup \beta$ for brevity. We give an example of the cohomology ring of the complex projective space.

Example 2.3.9. Since the complex projective space $\mathbb{CP}^n$ has a cell decomposition

$$\mathbb{CP}^n = \mathbb{C}^n \cup \mathbb{C}^{n-1} \cup \cdots \cup \mathbb{C}^0,$$

the cohomology $H^i(\mathbb{CP}^n, \mathbb{Z})$ is given by

$$H^i(\mathbb{CP}^n, \mathbb{Z}) = \begin{cases} \mathbb{Z} & \text{if } i = 0, 2, \cdots, 2n, \\ 0 & \text{otherwise.} \end{cases}$$

Let α_i be a generator of $H^{2i}(\mathbb{CP}^n, \mathbb{Z})$, which is Poincaré dual to a general complex projective subspace $\mathbb{CP}^{n-i}$ of $\mathbb{CP}^n$. By the property (2.6), we can check that

$$\alpha_i \cup \alpha_j = \begin{cases} \alpha_{i+j} & \text{if } i + j \leq n, \\ 0 & \text{otherwise.} \end{cases}$$

Therefore, the cohomology ring $H^*(\mathbb{CP}^n, \mathbb{ZZ})$ is isomorphic to the ring

$$\mathbb{Z}[\alpha]/\langle \alpha^{n+1} \rangle.$$

In particular, we consider the case that X is connected and $k + \ell = n$, i.e. $[Y \cap Z] \in H_0(X, \mathbb{Z}) \cong \mathbb{Z}$. Then $Y \cap Z$ is the set of finite points, each point has positive or negative orientation. For a point $P \in Y \cap Z$, we define by the intersection index

$$i_P(Y, Z) := \begin{cases} +1, & \text{if } P \text{ has a positive orientation,} \\ -1, & \text{if } P \text{ has a positive orientation.} \end{cases}$$

Then the number $[Y \cap Z] \in \mathbb{Z}$ is nothing but the sum of intersection indices taken over all points in $Y \cap Z$, which is called the intersection number. We note that the intersection number may be different from the actual number of intersection points because they are same only when all the intersection indices are $+1$. For instance, let X be a compact connected complex manifold and Y and Z be compact complex submanifolds of X such that they intersect transversely and the sum of codimensions of Y and Z is exactly the dimension of X. Then $Y \cap Z$ defines a zero cycle in $H_0(X, \mathbb{Z}) \cong \mathbb{Z}$ and all the intersection points has positive orientation, so the intersection number the number $[Y \cap Z] \in \mathbb{Z}$ is exactly the actual number of intersection points. However, we can not expect the same fortune for the general case.

2.4 Smooth varieties

For an irreducible polynomial f in $\mathbb{C}[x_1, \cdots, x_n]$, let us consider a hypersurface $Z(f)$ in the affine space $\mathbb{A}^n$. We choose a point $P = (a_1, \cdots, a_n)$ in X. Then we have known that the tangent space of X at P is given by the equation

$$\sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(P)(x_i - a_i) = 0$$

from the freshman calculus course. This is exactly the linear part of f, denoted by $f_P^{(1)}$, when we expand f at the point P by the Taylor expansion. Keeping in mind this, we define the tangent space of an affine variety.

Definition 2.4.1. Let X be an affine variety in $\mathbb{A}^n$ and $P = (a_1, \cdots, a_n)$ a point in X. Then the tangent space of X at the point P is defined by the intersection of all the tangent spaces of $Z(f)$ at P for all $f \in I(X)$, i.e.

$$T_P X := \bigcap_{f \in I(X)} Z(f_P^{(1)}) = Z(I(X)_P^{(1)}),$$

where $I(X)_P^{(1)}$ is the ideal generated by $f_P^{(1)}$ for every $f \in I(X)$.

As a matter of fact, the intersection in the definition above is the finite intersection of tangent spaces of $Z(f)$ for some $f \in I(X)$: If the ideal $I(X)$ is generated by some polynomials $f_1, \cdots, f_s$ in $\mathbb{C}[x_1, \cdots, x_n]$, then we can easily check that the tangent space $T_P X$ is noting but

$$\bigcap_{j=1}^{s} Z((f_j)_P^{(1)}).$$

Now, we introduce another kind of notion giving us a more refined picture of the local geometry of X. Let f be a polynomial in $\mathbb{C}[x_1, \cdots, x_n]$. By the Taylor expansion of f at a point P, we can write

$$f = \sum_{d \geq 0} f_P^{(d)},$$

where $f_P^{(d)}$ is the degree d part of the Taylor expansion of f at P. we define by $\mathtt{init}(f) = f_P^{(d)}$, called the initial polynomial of f, where d is the smallest number with nonzero $f_P^{(d)}$.

Definition 2.4.2. Let $X \subset \mathbb{A}^n$ be an affine variety and $P = (a_1, \cdots, a_n)$ a point in X. Then the tangent cone of X at the point P is defined by

$$C_P X := \bigcap_{f \in I(X)} Z\left(\mathtt{init}(f)\right) = Z(I(X)_{\mathtt{init}}),$$

where $I(X)_{\mathrm{init}}$ is the ideal generated by the initial ideals of $f \in I(X)$.

In the same way as in a tangent space, the tangent cone is actually the finite intersection of the form $Z(\mathrm{init}(f))$ for $f \in I(X)$: If the ideal $I(X)$ is generated by some polynomials $f_1, \cdots, f_s$ in $\mathbb{C}[x_1, \cdots, x_n]$, then the tangent cone $C_P X$ is

$$\bigcap_{j=1}^{s} Z(\mathrm{init}(f_j)).$$

Definition 2.4.3. Let P be a point in an affine variety $X \subset \mathbb{A}^n$. X is called smooth at the point P if $T_P X = C_P X$. Otherwise, it is called singular at P.

Now, let us consider the projective case. Since smoothness is a local property, it is reasonable that we define the notions above affine locally.

Definition 2.4.4. Let X be a projective variety in $\mathbb{P}^n$. For a point $P \in X$, we choose an affine open subset U of X containing the point P. Then X is smooth at the point P if the affine variety U is smooth at P. The tangent space $T_P X$ and the tangent cone $C_p X$ at the point $P \in X$ are defined by $T_P U$ and $C_P U$ respectively.

Practically, it is useful to choose an affine chart $U_i = \{x_i \neq 0\}$ of $\mathbb{P}^n$ containing the point P when we take an affine open subset of X. Then $X \cap U_i$ can be considered as an affine variety in $U_i \cong \mathbb{A}^n$, so we can apply the definition above more precisely. A variety X is called a smooth variety if it is smooth at every point $P \in X$. Otherwise, it is called a singular variety.

In fact, the definitions above of smoothness, a tangent space and a tangent cone never look intrinsic; it depends on the choice of polynomials of $I(X)$ and the choice of an affine neighborhood for the projective case. However, those notions of a variety are evidently intrinsic and we can define them intrinsically as well. However, the definitions above are enough for practical purposes. See [Har77, Chapter I, Section 5] for more details.

Example 2.4.5. Let $f(x, y) = y^2 - x^2 - x^3$ be a polynomial in $\mathbb{C}[x, y]$. Let X be a curve defined by f, i.e. $X = Z(y^2 - x^2 - x^3) \subset \mathbb{A}^2$. Since

$$\frac{\partial f}{\partial x}(P) = 0, \quad \frac{\partial f}{\partial y}(P) = 0$$

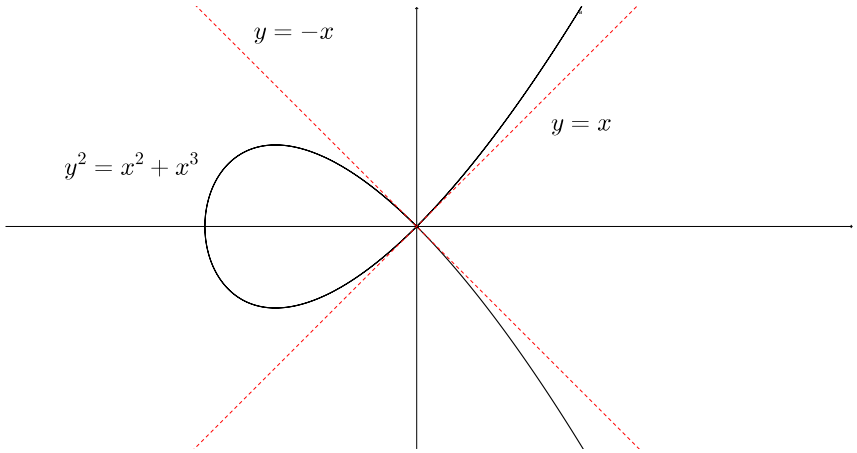

Figure 2.1: Nodal curve: $y^2 = x^2 + x^3$

for the origin $P = (0, 0)$, the tangent space at P is

$$T_P X = \left\{ (x, y) \in \mathbb{C}^2 \;\middle|\; \frac{\partial f}{\partial x}(P)x + \frac{\partial f}{\partial y}(P)y = 0 \right\} = \mathbb{C}^2.$$

On the other hand, the initial polynomial of f is $y^2 - x^2$, so the tangent cone of X is

$$C_P X = Z(y^2 - x^2).$$

The tangent cone is the union of two lines $\{y = x\}$ and $\{y = -x\}$. See Figure 2.1. The origin is a singular point of the curve X because the tangent space and the tangent cone does not coincide.

We note that for every polynomial f vanishing at the point P, its linear part $f_P^{(1)}$ is the initial polynomial of f whenever it is not zero. Hence $I(X)_P^{(1)}$ is contained in $I(X)_{\mathrm{init}}$, so

$$C_P X = Z(I(X)_{\mathrm{init}}) \;\subset\; Z(I(X)_P^{(1)}) = T_P X.$$

Moreover, it is well-known that the projectivized the tangent cone $\mathbb{P}(C_P X)$ of X at P is nothing but the exceptional divisor of the blow-up $\mathrm{Bl}_P X$ of X at

P [Har92, Lecture 20]. This fact implies that the dimension of the tangent cone $C_P X$ is exactly same as that of X itself when X is irreducible. Hence, we obtain

$$\dim X = \dim C_P X \leq \dim T_P X.$$

Therefore, a point P in an irreducible variety X is singular if and only if $\dim T_p X > \dim X$ by Definition 2.4.3. In practice, it is, however, cumbersome to calculate the tangent space and the tangent cone of X whenever we check smoothness of the variety X. The following criterion gives us a more efficient way to determine smoothness.

Theorem 2.4.6 (Jacobi criterion)**.** *Let X be an irreducible affine variety in $\mathbb{A}^n$. The ideal $I(X)$ is generated by some polynomials $f_1, \cdots, f_s$ in $\mathbb{C}[x_1, \cdots, x_n]$. The variety X is smooth at a point $P \in X$ if and only if the rank of the Jacobian matrix*

$$\begin{pmatrix} \frac{\partial f_1}{\partial x_1}(P) & \cdots & \frac{\partial f_1}{\partial x_n}(P) \\ \vdots & \ddots & \vdots \\ \frac{\partial f_s}{\partial x_1}(P) & \cdots & \frac{\partial f_s}{\partial x_n}(P) \end{pmatrix}$$

is $n - \dim X$.

Proof. X is smooth at a point P if and only if $\dim T_P X = \dim X$. Since the tangent space $T_P X$ is $\bigcap_{j=1}^{s} Z((f_j)_P^{(1)})$ and $f_j)_P^{(1)} = \sum_{i=1}^{n} \frac{\partial f_j}{\partial x_i}(P)(x_i - a_i)$, the Jacobian matrix has rank $n - \dim X$ is equivalent that codimension of the tangent space $T_P X$ is $n - \dim X$, i.e. $\dim T_P X = \dim X$. □

We note that the Jacobian matrix $\left(\frac{\partial f_i}{\partial x_j}(P)\right)$ at P has rank less than $n - \dim X$ if and only if the point P is a singular point of X. The condition that the rank of the Jacobian matrix is less than $n - \dim X$ is the Zariski closed condition because it is equivalent to the condition that all the $(n - \dim X) \times (n - \dim X)$ minors are zero. So, we can obtain the following.

Theorem 2.4.7. *Let X be a variety. Then the set of singular points of X is a proper closed subset of X.*

Before closing this section, we introduce another kind of tangent spaces. Let X be a projective variety in $\mathbb{P}^n$ and P a point in X. Let us consider the

affine cone $\widehat{X} \subset \mathbb{A}^{n+1}$ over X and choose a point $\widehat{P}$ over P, i.e. $\widehat{P} \in \pi^{-1}(P)$, where $\pi : \widehat{X} - \{0\} \longrightarrow X$ is the canonical projection map. We note that the tangent space $T_{\widehat{P}}\widehat{X}$ of $\widehat{X}$ at $\widehat{P}$ is a subspace of $\mathbb{A}^{n+1}$ passing through the origin and $\widehat{P}$, so the tangent space is invariant under the choice of the point $\widehat{P}$ in $\pi^{-1}(P)$. So, we can define by $\widehat{T}_P X$ the projectivization of the tangent space $T_{\widehat{P}}\widehat{X}$, i.e. $\mathbb{P}(T_{\widehat{P}}\widehat{X})$. This is called the embedded tangent space of X at the point P.

2.5 Grassmann varieties

Let V be a complex vector space of dimension n. Let $\mathrm{Gr}(k, V)$ denotes the set of all subspaces of codimension k. For a subspace W of V of codimension k, we denote by $[W]$ in $\mathrm{Gr}(k, V)$ the element represented by W. Let us take a basis $w_1, w_2, \cdots, w_{n-k}$ of W. Then we define a map

$$\begin{array}{ccc} \phi : \mathrm{Gr}(k, V) & \longrightarrow & \mathbb{P}(\bigwedge^{n-k} V). \\ [W] & \mapsto & [w_1 \wedge \cdots \wedge w_{n-k}] \end{array}$$

Then this is well-defined: If we choose another basis $w'_1, w'_2, \cdots, w'_{n-k}$ of W, then $w_1 \wedge \cdots \wedge w_{n-k}$ and $w'_1 \wedge \cdots \wedge w'_{n-k}$ differ by nonzero constant, so they represent the same point in the projective space $\mathbb{P}\left(\bigwedge^{n-k} V\right)$.

Moreover, the map ϕ is injective: It is enough to verify that any point $v = [w_1 \wedge \cdots \wedge w_{n-k}]$ in the image of ϕ, we can recover the subspace W of V such that $\phi([W]) = v$ uniquely . We can check that the subspace W is exactly determined as $\{w \in V \mid w \wedge v = 0\}$. Hence ϕ is injective. In fact, the image of ϕ is a projective variety whose defining equations are given by the so called the Plücker relations [GH11, Chapter 1, Section 5]. The morphism ϕ is called the Plücker embedding.

We fix a basis for V, so $V \cong \mathbb{C}^n$. In this case, We write $\mathrm{Gr}(k, n)$ for $\mathrm{Gr}(k, V)$. For a point $[W] \in \mathrm{Gr}(k, n)$, if we choose a basis $w_1, \cdots, w_{n-k}$ for W, then we can make the $(n-k) \times n$ matrix, called a matrix representation

of W,

$$\begin{pmatrix} \text{——} & w_1 & \text{——} \\ \text{——} & w_2 & \text{——} \\ & \vdots & \\ \text{——} & w_{n-k} & \text{——} \end{pmatrix}.$$

This matrix has full rank. Any $(n-k)\times n$ matrix of full rank represents an element in $\mathrm{Gr}(k,n)$ and two such matrices represent the same point of $\mathrm{Gr}(k,n)$ if and only if they differ by the left multiplication by a matrix in $\mathrm{GL}(n-k)$.

Let I be a subset of $\{1,2,\cdots,n\}$ with $|I| = n-k$. For an $(n-k)\times n$ matrix M, the determinant of the submatrix M_I, called I-th submatrix, of M selecting the columns whose indices belonging to I is called the I-th minor. Let U_I be the set of elements in $\mathrm{Gr}(k,n)$ whose matrix representations have the property that I-th minor does not vanish. Since for any matrix representation of an element in $\mathrm{Gr}(k,n)$, it has full rank, so there is an $(n-k)\times(n-k)$ submatrix whose determinant does not vanishes. Therefore, all the U_I cover the Grassmann variety.

$$\mathrm{Gr}(k,n) = \bigcup_{\substack{I\subset\{1,2,\cdots,n\}\\ |I|=n-k}} U_I.$$

For $[W]\in U_I$, its matrix representation M^W has an invertible $(n-k)\times(n-k)$ submatrix M_I^W. Then the I-th submatrix of $(M_I^W)^{-1}\cdot M^W$ is the identity matrix. Moreover, this form is unique for each element in U_I. Hence, it has $k(n-k)$ free variables. For instance, if $I=\{k+1,\cdots,n\}$, then all the element of U_I have the unique matrix representation of the following form.

$$\begin{pmatrix} w_{1,1} & \cdots & w_{1,k} & 1 & 0 & \cdots & 0 \\ w_{2,1} & \cdots & w_{2,k} & 0 & 1 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \ddots & \ddots & \vdots \\ w_{n-k,1} & \cdots & w_{n-k,k} & 0 & \cdots & 0 & 1 \end{pmatrix}, \tag{2.7}$$

This implies $U_I \cong \mathbb{C}^{k(n-k)}$. Since we can check that all the transitions from

U_I to U_J are holomorphic, $U_I \cong \mathbb{C}^{k(n-k)}$ form a chart of $\mathrm{Gr}(k,n)$, which means that $\mathrm{Gr}(k,n)$ is a complex manifold of dimension $k(n-k)$.

The Grassmann manifold has the so called universal bundle. Let $\mathrm{Gr}(k,n)\times\mathbb{C}^n$ be the trivial vector bundle of rank n over $\mathrm{Gr}(k,n)$. We define the universal bundle $\mathcal{U}$ over $\mathrm{Gr}(k,n)$ to be the subbundle of the trivial bundle $\mathrm{Gr}(k,n)\times\mathbb{C}^n$ whose fibers at each point $[W]\in\mathrm{Gr}(k,n)$ are exactly the subspace W of $\mathbb{C}^n$. Over a chart U_I of $\mathrm{Gr}(k,n)$, the matrix representation of the form (2.7) gives the frame of $\mathcal{U}$. From this, we can check that this is indeed the holomorphic subbundle of the trivial bundle $\mathrm{Gr}(k,n)\times\mathbb{C}^n$.

2.6 Segre varieties

Let V and W be the two vector spaces of dimension m and n respectively. Then the Segre variety is defined by the image of the following map

$$\begin{array}{rccc} Seg & : & \mathbb{P}V\times\mathbb{P}W & \longrightarrow & \mathbb{P}(V\otimes W). \\ & & ([x],[y]) & \mapsto & [x\otimes y] \end{array}$$

We choose and fix bases for V and W. Then vectors in V and W can be written in terms of the coordinates, i.e. $x=(x_1,\cdots,x_{m)}$ and $y=(y_1,\cdots,y_n)$. If we represent the coordinates of $V\otimes W$ as $(z_{i,j})$ for $1\le i\le m, 1\le j\le n$, then the vector $x\otimes y$ exactly corresponds to the coordinates (x_iy_j). Thus the map Seg can be expressed in terms of the coordinates as follows:

$$\begin{array}{rccc} Seg & : & \mathbb{P}^{m-1}\times\mathbb{P}^{n-1} & \longrightarrow & \mathbb{P}^{mn-1}. \\ & & ([x_i],[y_j]) & \mapsto & [x_iy_j] \end{array}$$

Hence the map Seg is a morphism of projective varieties. Since $(x_iy_j)(x_ky_l)=(x_iy_l)(x_ky_j)$ for every $1\le i,k\le m$ and $1\le j,l\le n$, the image of the Segre embedding is contained in the zero locus of the homogeneous quadratic polynomials

$$z_{i,j}z_{k,l}-z_{i,l}z_{j,k} \tag{2.8}$$

for $1 \leq i, k \leq m$ and $1 \leq j, l \leq n$. Moreover, we can easily check that if the quadratic polynomials in (2.8) vanish for all the $z_{i,j}$, there are x_i and y_j such that $z_{i,j} = x_i y_j$. So, the image of Seg is exactly defined by the polynomials in (2.8). Therefore, the image of Seg is indeed a projective variety, which is called the Segre variety. In fact, ϕ is a closed embedding, i.e. it is an isomorphism onto its image, so it is called the Segre embedding.

If we can think of the space $\mathbb{P}(V_1 \otimes V_2)$ as the projectivization of the vector space of $\dim V_1 \times \dim V_2$ matrices, then the Segre variety $Seg(\mathbb{P}V_1 \times \mathbb{P}V_2)$ becomes the set of all rank one matrices.

In the same way, we can directly generalize the definition of the Segre variety for more given vector spaces. Let $V_1, V_2, \cdots, V_r$ be vector spaces. The Segre map is defined by

$$\begin{array}{rccc} Seg & : & \mathbb{P}V_1 \times \mathbb{P}V_2 \times \cdots \times \mathbb{P}V_r & \longrightarrow & \mathbb{P}(V_1 \otimes V_2 \otimes \cdots \otimes V_r). \\ & & ([x_1], [x_2], \cdots, [x_r]) & \mapsto & [x_1 \otimes x_2 \otimes \cdots \otimes x_r] \end{array}$$

As for the case of two vector spaces, the map Seg is an embedding as well as a morphism of projective varieties. The image of Seg is called the Segre variety. The Segre variety $Seg(\mathbb{P}V_1 \times \cdots \times \mathbb{P}V_r)$ is, in general, also defined by the zero locus of some quadratic polynomials as for the case $r = 2$. The Segre variety $Seg(\mathbb{P}V_1 \times \cdots \times \mathbb{P}V_r)$ is the set of all rank one tensors in $\mathbb{P}(V_1 \otimes \cdots \otimes V_r)$. From the quantum information point of view, it is nothing but the set of pure separable states in $\mathbb{P}(V_1 \cdots \otimes V_r)$.

A Segre variety has an explicit description of its tangent space. The following lemma inform us what the tangent space is.

Lemma 2.6.1. *Let X be the Segre variety $Seg(\mathbb{P}V_1 \times \cdots \times \mathbb{P}V_r)$ and $[\mathbf{v}] = [\mathbf{v}_1 \otimes \cdots \otimes \mathbf{v}_r]$ a point of the variety. Then the embedded tangent space $T_{[\mathbf{v}]}X$ is*

$$\mathbb{P}(V_1 \otimes \mathbf{v}_2 \otimes \cdots \otimes \mathbf{v}_r + \mathbf{v}_1 \otimes V_2 \otimes \cdots \otimes \mathbf{v}_r + \cdots + \mathbf{v}_1 \otimes \mathbf{v}_2 \otimes \cdots \otimes V_r)$$

Proof. Let $\mathbf{v}(t) = \mathbf{v}_1(t) \otimes \cdots \otimes \mathbf{v}_r(t)$ be a smooth curve in the cone $\widehat{X}$ over

X with $\mathbf{v}(0) = \mathbf{v}$. By Leibniz's rule,

$$\mathbf{v}'(0) = \mathbf{v}_1'(0) \otimes \mathbf{v}_2 \otimes \cdots \otimes \mathbf{v}_r + \mathbf{v}_1 \otimes \mathbf{v}_2'(0) \cdots \otimes \mathbf{v}_r + \cdots + \mathbf{v}_1 \otimes \cdots \otimes \mathbf{v}_r'(0).$$

Since $\mathbf{v}_i'(0)$ can be chosen any, the set of all tangent vectors is

$$T_{\mathbf{v}}\widehat{X} = V_1 \otimes \mathbf{v}_2 \otimes \cdots \otimes \mathbf{v}_r + \mathbf{v}_1 \otimes V_2 \otimes \cdots \otimes \mathbf{v}_r + \cdots + \mathbf{v}_1 \otimes \mathbf{v}_2 \otimes \cdots \otimes V_r.$$

By projectivization, this proves the lemma. □

Now, let us calculate the degree of a Segre variety. Let $X = Seg(\mathbb{P}^m \times \mathbb{P}^n)$ be the Segre variety in $\mathbb{P}^{mn-1}$. By definition 2.3.6, the degree of X is determined by the leading coefficient of the Hilbert polynomial of X. We note that the restriction of a polynomial of degree d in $\mathbb{P}^{mn-1}$ to the Segre variety X is a bihomogeneous polynomial of degree (d, d) on $\mathbb{P}^m \times \mathbb{P}^n$. So,

$$\begin{aligned} h_X(d) &= h_{\mathbb{P}^m}(d) \cdot h_{\mathbb{P}^n}(d) \\ &= \binom{d+m}{m} \cdot \binom{d+n}{n} \\ &= \left(\frac{1}{m!}d^m + O(d^{m-1})\right)\left(\frac{1}{n!}d^n + O(d^{n-1})\right) \\ &= \frac{(m+n)!}{m!n!} \cdot \frac{1}{(m+n)!}d^{m+n} + O(d^{m+n-1}). \end{aligned}$$

Hence, the degree of the Segre variety $Seg(\mathbb{P}^m \times \mathbb{P}^n)$ is

$$\frac{(m+n)!}{m!n!}.$$

More generally, the Hilbert polynomial of the Segre variety $X = Seg(\mathbb{P}^{n_1} \times$

$\cdots \times \mathbb{P}^{n_r}$) is

$$\begin{aligned} h_X(d) &= \prod_{i=1}^{r} h_{\mathbb{P}^{n_i}}(d) \\ &= \prod_{i=1}^{r} \binom{d+n_i}{n_i} \\ &= \prod_{i=1}^{r} \left(\frac{1}{(n_i)!} d^{n_i} + O(d^{n_i-1}) \right) \\ &= \frac{(\sum_{i=1}^{r} n_i)!}{\prod_{i=1}^{r}(n_i)!} \cdot \frac{1}{(\sum_{i=1}^{r} n_i)!} d^{\sum_{i=1}^{r} n_i} + O(d^{\sum_{i=1}^{r} n_i - 1}) \end{aligned}$$

in the same way as in the case of two projective spaces. Therefore, the degree of the Segre variety $X = Seg(\mathbb{P}^{n_1} \times \cdots \times \mathbb{P}^{n_r})$ is

$$\frac{(\sum_{i=1}^{r} n_i)!}{\prod_{i=1}^{r}(n_i)!}.$$

Before closing this section, we describe the cohomology ring of the product of projective spaces. By Example 2.3.9, the cohomology ring of the complex projective space $\mathbb{P}^{m-1}$ is given by

$$H^*(\mathbb{P}^{m-1}, ZZ) = \mathbb{Z}[\alpha]/\langle \alpha^m \rangle.$$

By Künneth formula in algebraic topolgy [Hat02, Theorem 3.16], the cohomology ring of $\mathbb{P}^{m-1} \times \mathbb{P}^{n-1}$ is the tensor product of the cohomology rings of $\mathbb{P}^{m-1}$ and $\mathbb{P}^{n-1}$. Hence,

$$H^*(\mathbb{P}^{m-1} \times \mathbb{P}^{n-1}, \mathbb{Z}) \cong \mathbb{Z}[\alpha, \beta]/\langle \alpha^m, \beta^n \rangle.$$

Inductively, we can obtain the cohomology ring of $\mathbb{P}^{d_1-1} \times \cdots \times \mathbb{P}^{d_n-1}$ as follows:

$$H^*(\mathbb{P}^{d_1-1} \times \cdots \times \mathbb{P}^{d_n-1}, \mathbb{Z}) \cong \mathbb{Z}[\alpha_1, \cdots, \alpha_n]/\langle \alpha_1^{d_1}, \cdots, \alpha_n^{d_n} \rangle.$$

2.7 Join varieties, secant varieties and tangential varieties

Let X and Y be projective varieties in $\mathbb{P}^n$. For distinct two points x and y in $\mathbb{P}^n$, we denote by $\mathbb{P}^1_{xy}$ the line in $\mathbb{P}^n$ passing through x and y.

Definition 2.7.1. The join variety $J(X,Y)$ of X and Y to be the Zariski closure of the union of lines $\mathbb{P}^1_{xy}$ for every $x \in X$, $y \in Y$, i.e.

$$J(X,Y) := \overline{\bigcup_{x\in X,\ y\in Y,\ x\neq y} \mathbb{P}^1_{xy}}$$

Indeed, this is a variety: Let Δ_Y be a variety defined by

$$\Delta_Y := (X \times Y) \cap \Delta_X,$$

where Δ_X is the diagonal in $X \times X$. We define $\mathcal{J}^\circ_{X,Y}$ by

$$\mathcal{J}^\circ_{X,Y} := \{(x,y,z) \in (X \times Y)\backslash\Delta_Y \times \mathbb{P}^n \mid z \in \mathbb{P}^1_{xy}\}$$

and $\mathcal{J}_{X,Y}$ is its Zariski closure in $X\times Y\times\mathbb{P}^n$, then $\mathcal{J}_{X,Y}$ is an incidence variety. When we consider the natural projections

$$\begin{array}{ccc} & \mathcal{J}_{X,Y} & \\ {\scriptstyle p}\swarrow & & \searrow{\scriptstyle q} \\ X \times Y & & \mathbb{P}^n \end{array} \tag{2.9}$$

it is easily checked that $J(X,Y) = q(\mathcal{J}_{X,Y})$, so we can define $J(X,Y)$ by $q(\mathcal{J}_{X,Y})$ as a variety.

In particular, if $X = Y$, the join variety $\mathcal{J}(X,X)$ is called a secant variety of X, denoted by $\sigma(X)$. More generally, we can define the join of k varieties inductively by the argument above.

Definition 2.7.2. Let $X_1, X_2, \cdots, X_k$ be projective varieties in $\mathbb{P}^n$. We define

by the join variety of $X_1, X_2, \cdots, X_k$

$$J(X_1, X_2, \cdots, X_k) := J(X_1, J(X_2, \cdots, X_k))$$

by induction. In particular, if $X_1 = \cdots = X_k$, the join variety $J(X, \cdots, X)$ of k copies of X is called a k-secant variety, denoted by $\sigma_k(X)$.

We note that

$$J(X_1, \cdots, X_k) = \overline{\bigcup_{\substack{x_i \in X_i \\ x_i \text{ are linearly independent}}} \mathbb{P}_{x_1, \cdots, x_k}}, \tag{2.10}$$

where $\mathbb{P}_{x_1, \cdots, x_k}$ is the $(k-1)$-dimensional projective space spanned by $x_1, \cdots, x_k$.

Now, we introduce the notions of a rank or a border rank of a tensor. Those are deeply in connection with join varieties and secant varieties.

Definition 2.7.3. Let $V_1, V_2, \cdots, V_r$ be vector spaces and $\mathbf{t}$ an element of the tensor product $V_1 \otimes V_2 \otimes \cdots \otimes V_r$. We defined the rank of $\mathbf{t}$ is the minimum number s such that $\mathbf{t}$ can be written as

$$\mathbf{t} = \sum_{k=1}^{s} \mathbf{v}_1^{(k)} \otimes \mathbf{v}_2^{(k)} \otimes \cdots \otimes \mathbf{v}_r^{(k)},$$

where the vectors $\mathbf{v}_i^{(k)}$ are elements of V_i for each $1 \leq i \leq r$. We denote by $\mathrm{Rk}(\mathbf{t})$ the rank of the tensor $\mathbf{t}$.

Let X be the Segre variety $\mathrm{Seg}(\mathbb{P}^{n_1} \times \cdots \times \mathbb{P}^{n_r})$. We have known that it is the projectivization of the set of all rank one tensors in $\mathbb{C}^{n_1+1} \otimes \cdots \otimes \mathbb{C}^{n_r+1}$. By the description of the join variety in (2.10), the k-secant variety $\sigma_k(X)$ is exactly the closure of the projectivization of the set of all tensors in $\mathbb{C}^{n_1+1} \otimes \cdots \otimes \mathbb{C}^{n_r+1}$ whose ranks are less than or equal to k, i.e.

$$\sigma_k(\mathrm{Seg}(\mathbb{P}^{n_1} \times \cdots \times \mathbb{P}^{n_r})) = \overline{\mathbb{P}\left(\left\{\mathbf{t} \in \otimes_{i=1}^{r} \mathbb{C}^{n_i+1} \;\middle|\; \mathrm{Rk}(\mathbf{t}) \leq k\right\}\right)}.$$

We first consider the case $r = 2$. Let $V = \mathbb{C}^m \otimes \mathbb{C}^n$ be the tensor product of finite dimensional vector spaces and $\mathbf{t}$ an element of V. As we think of

the tensor $\mathbf{t}$ as an element of the set of all $m \times n$ matrices $\mathfrak{M}_{m,n} \cong \mathbb{C}^m \otimes \mathbb{C}^n$, we consider the usual rank of $\mathbf{t}$, denoted by $\mathrm{rk}(\mathbf{t})$. Suppose $\mathrm{rk}(\mathbf{t}) = \ell$. Then there are invertible matrices $A \in \mathrm{GL}(m)$ and $B \in \mathrm{GL}(n)$ such that

$$\mathbf{t} = A \left(\begin{array}{c|c} I_\ell & O \\ \hline O & O \end{array} \right) B.$$

Therefore, $\mathbf{t}$ can be written as the sum of ℓ rank one matrices, i.e. $\mathbf{t}$ is the sum of ℓ rank one tensors as an element of $\mathbb{C}^m \otimes \mathbb{C}^n$, so $\mathrm{Rk}(\mathbf{t}) \leq \mathrm{rk}(\mathbf{t})$. On the other hand, it is clear that $\mathrm{Rk}(\mathbf{t}) \geq \mathrm{rk}(\mathbf{t})$. If not, $\mathbf{t}$ can be expressed as the sum of less than $\mathrm{rk}(\mathbf{t})$ rank one tensors, then its rank as a $m \times n$ matrix never amount to $\mathrm{rk}(\mathbf{t})$. This is contradiction. As a result, the rank of tensors and that of a matrices are the same in the case $r = 2$. In this sense, the rank of a tensor can be regarded as a generalization of the rank of matrices.

In the case above, we note that the projectivization of the set of the $m \times n$ matrices whose ranks are less than or equal to k is a closed subvariety in $\mathbb{P}(\mathbb{C}^m \otimes \mathbb{C}^n)$ because it is exactly the zero locus of the polynomials given by $k \times k$ minors. Hence the k-secant variety $\sigma_k(\mathrm{Seg}(\mathbb{P}^{m-1} \times \mathbb{P}^{n-1}))$ is nothing but the projectivization of the set of the $m \times n$ matrices whose ranks are less than or equal to k, i.e.

$$\sigma_k(\mathrm{Seg}(\mathbb{P}^{m-1} \times \mathbb{P}^{n-1})) = \mathbb{P}\left(\{\mathbf{t} \in \mathbb{C}^m \otimes \mathbb{C}^n \mid \mathrm{Rk}(\mathbf{t}) \leq k\}\right).$$

We notice that we do not have to take the closure.

Now, we consider the case $r = 3$. It is natural that we wonder if taking the closure is necessary in this case as well. Unlike the case $r = 2$, the projectivization of the set of the tensors in $\mathbb{C}^\ell \otimes \mathbb{C}^m \otimes \mathbb{C}^n$ whose ranks are less than or equal to k is not necessarily closed.

Example 2.7.4. Let $\mathbf{e}_1, \mathbf{e}_2$ be a basis for $\mathbb{C}^2$. Then the tensor

$$\mathbf{t}_\epsilon = \frac{(\mathbf{e}_1 + \epsilon\mathbf{e}_2) \otimes (\mathbf{e}_1 + \epsilon\mathbf{e}_2) \otimes (\mathbf{e}_1 + \epsilon\mathbf{e}_2) - \mathbf{e}_1 \otimes \mathbf{e}_1 \otimes \mathbf{e}_1}{\epsilon}$$

in $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ has rank two for any $\epsilon \neq 0$, but the limit

$$\lim_{\epsilon \to 0} \mathbf{t}_\epsilon = \mathbf{e}_2 \otimes \mathbf{e}_1 \otimes \mathbf{e}_1 + \mathbf{e}_1 \otimes \mathbf{e}_2 \otimes \mathbf{e}_1 + \mathbf{e}_1 \otimes \mathbf{e}_1 \otimes \mathbf{e}_2$$

has rank three. In fact, the tensor $\mathbf{t}_\epsilon$ is a point on the secant line joining $\mathbf{e}_1 \otimes \mathbf{e}_1 \otimes \mathbf{e}_1$ and $(\mathbf{e}_1 + \epsilon\mathbf{e}_2) \otimes (\mathbf{e}_1 + \epsilon\mathbf{e}_2) \otimes (\mathbf{e}_1 + \epsilon\mathbf{e}_2)$ which are elements of the Segre variety $\mathit{Seg}(\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1)$. Hence, it is clear that the limit $\lim_{\epsilon \to 0} \mathbf{t}_\epsilon$ belongs to a tangent line at the point $\mathbf{e}_1 \otimes \mathbf{e}_1 \otimes \mathbf{e}_1$.

Under these observations, we define the notion of a border rank.

Definition 2.7.5. A tensor $\mathbf{t}$ has border rank s if it is a limit of tensors of rank s, but is not a limit of tensors of rank s' for $s' < s$. $\underline{\mathsf{Rk}}(\mathbf{t})$ denotes the border rank of $\mathbf{t}$.

It is obvious that $\underline{\mathsf{Rk}}(\mathbf{t}) \leq \mathsf{Rk}(\mathbf{t})$. By the definition of a secant variety, the k-secant variety of the Segre variety $\mathit{Seg}(\mathbb{P}^{n_1} \times \cdots \times \mathbb{P}^{n_r})$ is

$$\sigma_k(\mathit{Seg}(\mathbb{P}^{n_1} \times \cdots \times \mathbb{P}^{n_r})) = \mathbb{P}\left(\left\{\mathbf{t} \in \otimes_{i=1}^{r} \mathbb{C}^{n_i+1} \mid \underline{\mathsf{Rk}}(\mathbf{t}) \leq k\right\}\right).$$

In order to estimate the dimension of join varieties, we introduce a useful theorem, known as the Terracini's Lemma.

Theorem 2.7.6 (Terracini's Lemma)**.** *[FOV99, Proposition 4.3.2] Let X and Y be projective varieties in $\mathbb{P}^n$. For points $x \in X$, $y \in Y$ and $z \in \mathbb{P}^1_{xy}$,*

$$\widehat{T}_z J(X, Y) \supseteq \widehat{T}_x X + \widehat{T}_y Y.$$

Moreover, there is a nonempty dense open subset $\mathcal{U}$ of $J(X, Y)$ such that the equality holds for $x \in X$, $y \in Y$ and $z \in \mathcal{U} \cap \mathbb{P}^1_{xy}$.

Example 2.7.7. Let X be the Segre variety $Seg(\mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1)$. Let us calculate the dimension of $\sigma_2(X)$ taking advantage of the Terracini's lemma. We write $\mathbf{v} = \mathbf{x}_1 \otimes \mathbf{y}_1 \otimes \mathbf{z}_1 + \mathbf{x}_2 \otimes \mathbf{y}_2 \otimes \mathbf{z}_2$ for a general point $\widehat{\sigma_2(X)}$. We may assume that $\mathbf{x}_1$ and $\mathbf{x}_2$, $\mathbf{y}_1$ and $\mathbf{y}_2$, $\mathbf{z}_1$ and $\mathbf{z}_2$ are linearly independent respectively. Then

$$\begin{aligned}\widehat{T}_{[\mathbf{v}]}\sigma_2(X) =& \widehat{T}_{[\mathbf{x}_1\otimes\mathbf{y}_1\otimes\mathbf{z}_1]}X + \widehat{T}_{[\mathbf{x}_2\otimes\mathbf{y}_2\otimes\mathbf{z}_2]}X \\ =& \mathbb{P}(\mathbb{C}^2 \otimes \mathbf{y}_1 \otimes \mathbf{z}_1 + \mathbf{x}_1 \otimes \mathbb{C}^2 \otimes \mathbf{z}_1 + \mathbf{x}_1 \otimes \mathbf{y}_1 \otimes \mathbb{C}^2 \\ & + \mathbb{C}^2 \otimes \mathbf{y}_2 \otimes \mathbf{z}_2 + \mathbf{x}_2 \otimes \mathbb{C}^2 \otimes \mathbf{z}_2 + \mathbf{x}_2 \otimes \mathbf{y}_2 \otimes \mathbb{C}^2).\end{aligned}$$

In order to calculate the dimension of the last sum, we have to investigate the intersections of some of them. For instance, the intersection of $\mathbb{C}^2 \otimes \mathbf{y}_1 \otimes \mathbf{z}_1$ and $\mathbf{x}_1 \otimes \mathbb{C}^2 \otimes \mathbf{z}_1$ is the line spanned by $\mathbf{x}_1 \otimes \mathbf{y}_1 \otimes \mathbf{z}_1$, so its dimension is one. We can easily check that the intersections of two of the first three terms or the last three terms are one-dimensional. The intersections of the first three terms or the last three terms are also one-dimensional. Hence the dimension of the last sum is $2 \cdot 6 - 1 \cdot 6 + 1 \cdot 2 - 1 = 7$. Since $\sigma_2(X)$ is contained in $\mathbb{P}^7$, $\sigma_2(X)$ is the whole space $\mathbb{P}^7$.

Let us recall Example 2.7.4. We have seen that the limit $\lim_{\epsilon\to 0} \mathbf{t}_\epsilon$ lies on a tangent line at the point in the Segre variety. Keeping in mind this example, we define a tangential variety as follows.

Definition 2.7.8. Let $X \subset \mathbb{P}^n$ be a projective variety and Y a subvariety of X. We define by the variety of relative tangent stars of X with respect to the subvariety Y

$$T(X, Y) := q \circ p^{-1}(\Delta_Y)$$

in the diagram (2.9). In particular, we define $\tau(X) := T(X, X)$, which is called the tangential variety of X.

The geometric meaning of $T(X, Y)$ is clear from the diagram (2.9). it is the union of the tangent lines which are given by the limits of the secant lines $\mathbb{P}^1_{xy}$ as $x \in X$ and $y \in Y$ goes to a point in Y.

In general, the secant variety $\sigma(X)$ has the expected dimension $2\dim X+1$ because there are $\dim X$ degree of freedom for the choice of $x \in X$ and 1

degree of freedom for the choice of a point in $\mathbb{P}^1_{xy}$. On the other hand, the tangential variety $\tau(X)$ has the expected dimension $2\dim X$ because there are $\dim X$ degree of freedom for the choice of $x \in X$, $\dim X - 1$ degree of freedom for the choice of the direction of the tangent line and 1 degree of freedom for the choice of a point in the tangent line. Moreover, it is clear that $p^{-1}(\Delta_Y) \subset \mathcal{J}_{X,Y}$ in the diagram (2.9), the tangential variety $\tau(X)$ is contained in the secant variety $\sigma(X)$. The following theorem informs us that if the secant variety has no expected dimension, then the secant variety and the tangential variety coincide.

Theorem 2.7.9. *(Zak's Theorem on Tangencies)[Zak05, Theorem 1.4] Let X be an r-dimensional projective variety in $\mathbb{P}^n$. Then one of the following holds.*

(i) $\dim \sigma(X) = 2r + 1$ *and* $\dim \tau(X) = 2r$.

(ii) $\dim \sigma(X) = \dim \tau(X)$.

This result is one of the interesting applications of the Fulton-Hansen Connectedness Theorem [FH79]. See [Laz04, Section 3.4] for more details.

2.8 Dual varieties and hyperdeterminants

Hyperdeterminant is a higher-dimensional generalization of the determinant of a square matrix. Historically, there have been several definitions of multidimensional determinant [Mui03]. The most natural one was defined by Cayley [Cay45] in some special cases, Gelfand, Manin and Zelevinsky [GKZ92] generalize and formalize his method by means of modern language. In this section, we introduce the notion of dual varieties and that of hyperdeterminants in terms of dual varieties.

Let V be a finite dimensional vector space. We fix a basis for V and denote by V^* the dual space of V. Since an element of V^* is a linear form, $\mathbb{P}(V^*)$ can be regarded as the set of all hyperplanes in V. Let X be a projective variety in $\mathbb{P}^n$. A hyperplane H is said to be tangent to X if it contains the tangent space to X at a smooth point of X.

Definition 2.8.1. The dual variety $X^\vee$ in $\mathbb{P}(V^*)$ is defined by the Zariski closure of the set of all the hyperplanes tangent to X, i.e.

$$X^\vee := \{H \in \mathbb{P}(V^*) \mid \widehat{T}_x X \subset H \text{ for a smooth point } x \in X\}$$

This is indeed a variety: The proof is similar to the case for the join varieties. Let us consider the set

$$W^\circ := \{(x, H) \in \mathbb{P}^n \times (\mathbb{P}^n)^* \mid x \text{ is a smooth point of } X,\ \widehat{T}_x X \subset H\}$$

and let W be the Zariski closure of W°. This is called the incidence variety corresponding to X. We consider the natural two projections:

$$\begin{array}{ccccc} & & W & & \\ & \swarrow^{p} & & \searrow^{q} & \\ X \subset \mathbb{P}^n & & & & X^\vee \subset (\mathbb{P}^n)^* \end{array} \tag{2.11}$$

It is clear that $q(W) = X^\vee$, so $X^\vee$ is a projective variety. Moreover, if X is irreducible, so is $X^\vee$: Note that the restriction $p\big|_{W^\circ}$ makes W° a projective bundle over the smooth locus X_{sm} of X. This implies if X is irreducible, so are X_{sm}, W°. The closure W of W° and $q(W) = X^\vee$ are also irreducible.

Let us first consider a simple example. Let $C = Z(ax^2 + by^2 + cz^2)$ be a smooth conic curve in $\mathbb{P}^2$ for nonzero numbers $a, b, c \in \mathbb{C}$. For a point $P = (x_0, y_0, z_0) \in C$, The tangent line of C at P is given by

$$T_P C = \left\{[x : y : z] \in \mathbb{P}^2 \mid (ax_0, by_0, cz_0) \cdot (x, y, z) = 0\right\}.$$

Since a hyperplane containing $\widehat{T}_P C$ is unique and it is $\widehat{T}_P C$ itself, the dual variety $C^\vee$ is

$$\begin{aligned} C^\vee &= \left\{[ax : by : cz] \in \left(\mathbb{P}^2\right)^* \mid ax^2 + by^2 + cz^2 = 0\right\} \\ &= \left\{[X : Y : Z] \in \left(\mathbb{P}^2\right)^* \;\middle|\; \frac{X^2}{a} + \frac{Y^2}{b} + \frac{Z^2}{c} = 0\right\} \end{aligned}$$

Therefore, the dual variety $C^\vee$ is also a smooth curve in $\mathbb{P}^2$. Moreover, we can easily check that $(C^\vee)^\vee$ is the same as the original curve C itself.

In general, there is no reason to preserve the degree and the dimension of a variety under the dual operation. For instance, the dual of a point P is the set of all hyperplanes containing the point P, so they form a hyperplane in the dual projective space. Moreover, if C be a smooth curve of degree d in $\mathbb{P}^2$, its dual curve has degree $d(d-1)$ in general [GH11, Chapter 2, Section 4].

Example 2.8.2. Let X be the Segre variety $Seg(\mathbb{P}^n \times \mathbb{P}^n)$. Let $[x_i]$ and $[y_j]$ be the coordinates of $\mathbb{P}^n$ for $1 \leq i, j \leq n$. Then the Segre variety X has a parametric representation $[x_i y_j]$. Let

$$H = \left\{ [z_{ij}] \in \mathbb{P}^{(n+1)^2-1} \;\middle|\; L := \sum_{1 \leq i,j \leq n} a_{ij} z_{ij} = 0 \right\}$$

be the hyperplane in $\mathbb{P}^n$ determined by a linear form L. Then H is tangent to X if and only if after restricting L to X, it has a multiple root as a polynomial in x_i and y_j, i.e. there is a point $P \in \mathbb{P}^n \times \mathbb{P}^n$ such that

$$L|_X(P) = \frac{\partial L|_X}{\partial x_1}(P) = \cdots = \frac{\partial L|_X}{\partial x_n}(P) = \frac{\partial L|_X}{\partial y_1}(P) = \cdots = \frac{\partial L|_X}{\partial y_n}(P) = 0,$$

where $L|_X = \sum a_{ij} x_i y_j$. This condition is equivalent that the determinant of the $(n+1) \times (n+1)$ matrix $A := (a_{ij})$ vanishes, so the dual of the Segre variety $Seg(\mathbb{P}^n \times \mathbb{P}^n)$ is the hypersurface defined by the determinant.

Now, we claim that the dual of the dual variety $X^\vee$ is X itself. Since $X^\vee$ is the hypersurface, any hyperplane containing a tangent space to $X^\vee$ is the tangent space itself, so the dual of the dual variety $X^\vee$ has a parametric representation as follows:

$$(X^\vee)^\vee = \left\{ \left(\frac{\partial \det(A)}{\partial a_{11}} : \frac{\partial \det(A)}{\partial a_{12}} : \cdots : \frac{\partial \det(A)}{\partial a_{n+1,n+1}} \right) \in \mathbb{P}^{(n+1)^2-1} \right\}.$$

We can easily check that

$$\frac{\partial \det(A)}{\partial a_{k\ell}} = (-1)^{k+\ell} M_{k\ell},$$

where $M_{k\ell}$ is the (i,j)-minor, which is the determinant of the submatrix of A deleting the k-th row and the ℓ-th column. Let us consider the adjoint matrix $\operatorname{adj}(A) = \left((-1)^{k+\ell} M_{k\ell}\right)$. By the standard argument of linear algebra, we have known that

$$A \cdot \operatorname{adj}(A) = \det A \cdot I,$$

where I is the identity matrix. Since $\det A = 0$, the range of $\operatorname{adj} A$ is contained in the kernel of A, which has the dimension one. Hence, all the 2×2 minors of $\operatorname{adj} A$ should be zero, which is exactly the relations (2.8) defining the Segre variety. This proves the claim.

All the examples above we can expect the dual of the dual variety $X^\vee$ is the same as the variety X itself.

Theorem 2.8.3 (Biduality Theorem)**.** *[GKZ08, Theorem 1.1] Let X be an irreducible projective variety in $\mathbb{P}^n$. Then the dual of the dual variety $X^\vee$ is exactly the variety X itself, i.e.*

$$X^{\vee\vee} = X.$$

Moreover, if X is smooth at P and $X^\vee$ is smooth at H, the condition $T_P X \subset H$ is equivalent to the condition $T_H X^\vee \subset P$, considered as the hyperplane in $\mathbb{P}(V^*)$

From Example 2.8.2, we see that the dual of a Segre variety has an interesting connection with the determinant. The determinant of $(n+1)\times(n+1)$ matrix is nothing but the defining equation of the dual variety $\operatorname{Seg}(\mathbb{P}^n \times \mathbb{P}^n)^\vee$. The following theorem tells us the condition for which the dual of the Segre variety is a hypersurface.

Theorem 2.8.4. *[GKZ08, Chapter 14, Theorem 1.3] Let X be the Segre variety $\operatorname{Seg}(\mathbb{P}^{n_1} \times \cdots \times \mathbb{P}^{n_r})$. Then the dual variety $X^\vee$ is a hypersurface if and*

only if

$$n_i \leq \sum_{j \neq i} n_j$$

for every $i = 1, \cdots, r$.

For the case $r = 2$, the dual variety $\mathsf{Seg}(\mathbb{P}^m \times \mathbb{P}^n)^\vee$ is a hypersurface if and only if $m = n$. This is why we define the determinant of a matrix only when the matrix is a square one.

Keeping in mind these observations, we define the determinant of a higher dimensional matrix. Let $n_1, n_2, \cdots, n_r$ be positive integers. Let $a_{i_1,i_2,\cdots,i_r}$ be complex numbers for $0 \leq i_j \leq n_j$. Then $A = (a_{i_1,i_2,\cdots,i_r})$ is called an r-dimensional matrix of format $(n_1 + 1) \times (n_2 + 1) \times \cdots \times (n_r + 1)$ over $\mathbb{C}$.

Definition 2.8.5. Let $A = (a_{i_1,i_2,\cdots,i_r})$ be an r-dimensional matrix of format $(n_1 + 1) \times (n_2 + 1) \times \cdots \times (n_r + 1)$ over $\mathbb{C}$. Suppose that

$$n_i \leq \sum_{j \neq i} n_j$$

for every $i = 1, \cdots, r$. Then we define by the hyperdeterminant of A, denoted $\mathsf{Det}(A)$, the defining equation of the dual variety of $\mathsf{Seg}(\mathbb{P}^{n_1} \times \cdots \times \mathbb{P}^{n_r})$.

Since there is no canonical isomorphism between a vector space and its dual space, the above definition of the hyperdeterminant of a matrix seems to depend on the choice of the basis of the dual variety. However, it does not matter since the hyperdeterminant is invariant under the action of the group $\mathrm{SL}(n_1 + 1) \times \cdots \times \mathrm{SL}(n_r + 1)$ [GKZ08, Chapter 14, Proposition 1.4].

Although there are many ways known to calculate the hyperdeterminant of a matrix, it is in general hard to write down the form explicitly. For instance, the hyperdeterminant of a matrix of format $2 \times 2 \times 2 \times 2$ is a polynomial of degree 24 which has 2894276 terms [HSYY08]! In this section, we only introduce a method by Schläfli, which is a classical method to calculate the hyperdeterminant simply for some special cases.

Let A be a matrix of format $\ell \times m \times n$. Then it can be considered as a $m \times n$ matrix whose entries are elements in $\mathbb{C}^\ell$. If we change a basis for $\mathbb{C}^\ell$

into variables $\mathbf{x} = (x_1, \cdots, x_\ell)$, we can make the $m \times n$ matrix $\tilde{A}(\mathbf{x})$ whose entries are linear forms in $\mathbf{x}$.

Theorem 2.8.6. *[Ott13, Proposition 5.2] Let A be a matrix of format $m \times n \times n$. Then the hyperdeterminant of A divides the discriminant of $\det \tilde{A}(\mathbf{x})$. In particular, they are same for the case $m = 2$ or 3.*

Making use of this theorem, we can calculate the case $2 \times 2 \times 2$ explicitly.

Example 2.8.7 ($2\times2\times2$ case)**.** Let $A = (a_{ijk})$ be a matrix of format $2\times2\times2$. Then the matrix $\tilde{A}(\mathbf{x})$ is

$$\begin{pmatrix} a_{000}x_0 + a_{100}x_1 & a_{001}x_0 + a_{101}x_1 \\ a_{010}x_0 + a_{110}x_1 & a_{011}x_0 + a_{111}x_1 \end{pmatrix}$$

By Theorem 2.8.6, the discriminant of the determinant of the matrix above is the hyperdeterminant of A. The determinant of $\tilde{A}(\mathbf{x})$ is

$$\begin{aligned}\tilde{A}(\mathbf{x}) =&(a_{000}a_{011} - a_{001}a_{010})x_0^2 + (a_{000}a_{111} + a_{100}a_{011} - a_{001}a_{110} - a_{101}a_{010})x_0x_1 \\ &+ (a_{100}a_{111} - a_{101}a_{110})x_1^2,\end{aligned}$$

so its discriminant is

$$\begin{aligned}&(a_{000}a_{111} + a_{100}a_{011} - a_{001}a_{110} - a_{101}a_{010})^2 \\ -4&(a_{000}a_{011} - a_{001}a_{010})(a_{100}a_{111} - a_{101}a_{110})\end{aligned}$$

This is the hyperdeterminant of A.

2.9 Newton polytopes and Bernstein's theorem

A Newton polytope is a combinatorial object given by a polynomial. This notion plays a key role connecting between algebraic properties of polynomials and combinatorial ones. One of the interesting results is the so called Bernstein's theorem (Theorem 2.9.6), which describes the number of common roots of some polynomials in terms of the mixed volume of the New-

ton polytopes defined by the polynomials. We introduce related notions and theorems.

A polytope P is defined by the convex hull of a finite set $A \subset \mathbb{R}^n$. In particular, it is called a lattice polytope if $A \subset \mathbb{Z}^n$. Let P and Q be polytopes in $\mathbb{R}^n$ and λ a nonnegative real number. We define their sum and scalar multiple as follows:

(i) $P + Q = \{\, p + q \in \mathbb{R}^n \mid p \in P,\ q \in Q \,\}$, where $p + q$ is the usual sum of vectors in $\mathbb{R}^n$,

(ii) $\lambda P = \{\, \lambda p \in \mathbb{R}^n \mid p \in P \,\}$, where λp is the usual scalaar multiplication in $\mathbb{R}^n$.

Sometimes the sum of polytopes $P+Q$ is called the Minkowski sum of P and Q. We can directly generalize the definition of Minkowski sum and scalar multiple to the case for several polytopes.

Definition 2.9.1. Let P be a polytope in $\mathbb{R}^n$. We define by the n-dimensional volume $\mathrm{Vol}_n(P)$ of P the usual Euclidean volume, i.e.,

$$\mathrm{Vol}_n(P) := \int_P dx_1 \cdots dx_n.$$

This definition of volume is exactly the same as what we have known usually. However, we notice that if the polytope is contained in a real subspace $\mathbb{R}^{n-1}$ of $\mathbb{R}^n$, then $\mathrm{Vol}_n(P)$ is always zero. For instance, the 3-dimensional volume of a polygon, which is a two-dimensional polytope, is clearly zero.

For a polytope P in $\mathbb{R}^n$, let us consider the volume $\mathrm{Vol}_n(\lambda P)$ as a function in λ. Since the volume of λP is exactly the product of λ^n and $\mathrm{Vol}_n(P)$, $\mathrm{Vol}_n(\lambda P)$ is the degree n monomial function in λ with the coefficient $\mathrm{Vol}_n(P)$. How about the volume $\mathrm{Vol}_n(\lambda P + \mu Q)$ for two polytopes P and Q? The following theorem says that it is a homogeneous polynomial of degree n in λ and μ.

Theorem 2.9.2. *[CLO05, Chapter 7, Proposition 4.9] Let $P_1, P_2, \cdots, P_r$ be polytopes in $\mathbb{R}^n$. If we think of an n-dimensional volume $\mathrm{Vol}_n(\lambda_1 P_1 + \cdots +$*

$\lambda_r P_r$) *as a function in variables* λ_i*, then the volume* $\mathrm{Vol}_n(\lambda_1 P_1 + \cdots + \lambda_r P_r)$ *is indeed a homogeneous polynomial of degree* n *in the variables* λ_i.

For example, let us consider the volume $\mathrm{Vol}_2(\lambda P + \mu Q)$. By Theorem 2.9.2, it is a homogeneous polynomial $A\lambda^2 + B\lambda\mu + C\mu^2$ for some numbers A, B and C. When $\mu = 0$, we get $A = \mathrm{Vol}_2(P)$. In the same way, we obtain $B = \mathrm{Vol}_2(Q)$. What is the coefficient of $\lambda\mu$? We define it as the mixed volume of P and Q.

Definition 2.9.3. Let $P_1, P_2, \cdots, P_n$ be polytopes in $\mathbb{R}^n$. We define by the n-dimensional mixed volume $\mathrm{MV}_n(P_1, \cdots, P_n)$ of the polytopes $P_1, \cdots, P_n$ the coefficient of the monomial $\prod_{i=1}^n \lambda_i$ in the homogeneous polynomial function $\mathrm{Vol}_n(\lambda_1 P_1 + \cdots + \lambda_n P_n)$ in λ_i.

Let us continue investigating the example of $\mathrm{Vol}_2(\lambda P + \mu Q)$ above. When $\lambda = \mu$, $\mathrm{Vol}_2(\lambda P + \mu Q)$ turns into $\mathrm{Vol}_2(P + Q)\lambda^2$. On the other hand, the homogeneous polynomial $A\lambda^2 + B\lambda\mu + C\mu^2$ becomes $(A + B + C)\lambda^2$. Hence, the coefficient B of $\lambda\mu$ is

$$\mathrm{MV}_2(P, Q) = \mathrm{Vol}_2(P + Q) - A - B = \mathrm{Vol}_2(P + Q) - \mathrm{Vol}_2(P) - \mathrm{Vol}_2(Q).$$

This inclusion-exclusion like property also holds for higher dimensional cases.

Proposition 2.9.4. *[Ful93, Section 5.4]*

$$\mathrm{MV}_n(P_1, P_2, \cdots, P_n) = \sum_{k=1}^{n} (-1)^{n-k} \sum_{\substack{I \subset \{1, \cdots, n\} \\ |I| = k}} \mathrm{Vol}_n \left(\sum_{i \in I} P_i \right)$$

We notice that mixed volumes are always non-negative and monotone increasing with respect to inclusion, i.e.

$$\mathrm{MV}_n(P_1, P_2, \cdots, P_n) \geq \mathrm{MV}_n(P'_1, P'_2, \cdots, P'_n) \quad \text{if } P_i \supset P'_i \text{ for all } i.$$

Now, let us introduce the so called Newton polytope.

Definition 2.9.5. Let f be a Laurent polynomial in $\mathbb{C}[x_1^{\pm 1}, \cdots, x_n^{\pm 1}]$. The Newton polytope $New(f)$ of the polynomial f is defined by the convex hull of the exponents of terms of f whose coefficients are not zero, i.e.

$$New(f) := \mathrm{Conv}\left(\left\{\mathbf{a} \in \mathbb{Z}^n \;\middle|\; f = \sum c_{\mathbf{a}} \mathbf{x}^{\mathbf{a}},\ c_{\mathbf{a}} \neq 0\right\}\right).$$

Bernstein discovered a beautiful way to obtain algebraic information from combinatorial geometric objects. The statement is the following.

Theorem 2.9.6 (Bernstein's Theorem)**.** *[Ber75] Let $f_1, f_2, \cdots, f_n$ be Laurent polynomials in $\mathbb{C}[x_1^{\pm 1}, \cdots, x_n^{\pm 1}]$. If they have finitely many common roots in $(\mathbb{C}^*)^n$, then the number of common roots of $f_1, f_2, \cdots, f_n$ in $(\mathbb{C}^*)^n$ is less than or equal to the mixed volume of the Newton polytopes of $f_1, f_2, \cdots, f_n$, i.e.*

$$MV_n(New(f_1), New(f_2), \cdots, New(f_n)).$$

In the theorem above, we notice that the number of common roots is counted not in $\mathbb{C}^n$, but $(\mathbb{C}^*)^n$. This is essentially because the mixed volume is invariant under the translation of polytopes. A translation of Newton polytopes $New(f_i)$ correspond to a multiplication f_i by a monomial. If the polynomials f_i are multiplied by the same monomial, they have common roots in the origin, but their mixed volume does not change.

However, we sometimes would like to know how many common roots in $\mathbb{C}^n$ exist for some given polynomials. Li and Wang modified the Bernstein's results to the case allowing the entries of common roots to be zero.

Theorem 2.9.7. *[LW96] If polynomials $f_1, f_2, \cdots, f_n$ in $\mathbb{C}[x_1, x_2, \cdots, x_n]$ have finitely many common roots in $\mathbb{C}^n$, then the number of common roots in $\mathbb{C}^n$ is less than or equal to*

$$MV_n(\mathrm{Conv}(New(f_1) \cup \{0\}), \mathrm{Conv}(New(f_2) \cup \{0\}), \cdots, \mathrm{Conv}(New(f_n) \cup \{0\})),$$

where 0 is the origin.

We remark that Bernstein's theorem and the result of Li and Wang are in some sense a generalization of Bezout's theorem: Let f and g be polynomials

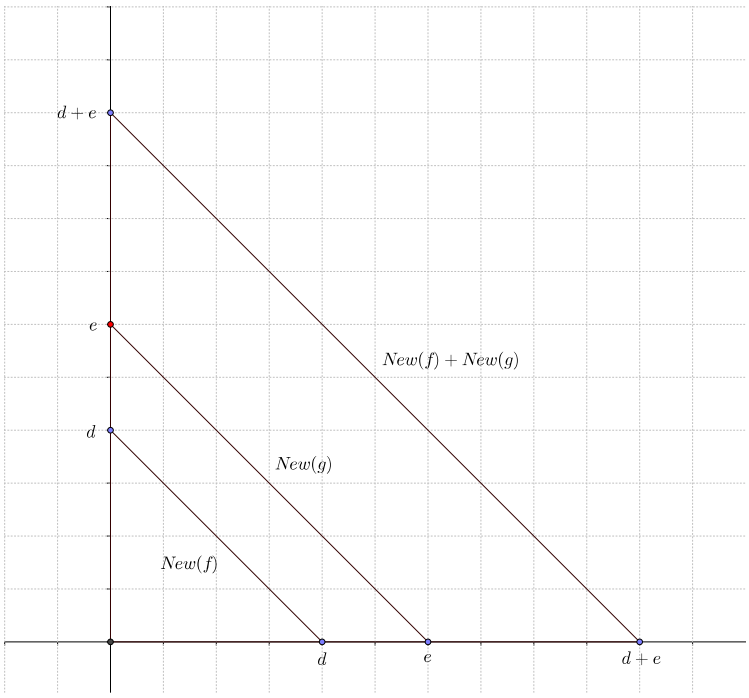

Figure 2.2: Newton polytopes of f and g

in $\mathbb{C}[x,y]$ of degree d and e respectively. Then the Newton polytopes of f and g are

$$\mathit{New}(f) = \mathrm{Conv}(\{(0,0),(d,0),(0,d)\}),$$
$$\mathit{New}(g) = \mathrm{Conv}(\{(0,0),(e,0),(0,e)\}).$$

Since both $\mathit{New}(f)$ and $\mathit{New}(g)$ contains the origin, $\mathrm{Conv}(\mathit{New}(f)\cup 0) = \mathit{New}(f)$ and $\mathrm{Conv}(\mathit{New}(g)\cup 0) = \mathit{New}(g)$. We can also readily check that the Minkowski sum $\mathit{New}(f)+\mathit{New}(g)$ is

$$\mathrm{Conv}(\{(0,0),(d+e,0),(0,d+e)\}).$$

See Figure 2.2. Hence, the mixed volume of $New(f)$ and $New(g)$ is

$$\begin{aligned} MV_2(New(f), New(g)) &= Vol_2(New(f) + New(g)) - Vol_2(New(f)) - Vol_2(New(g)) \\ &= \frac{1}{2}(d+e)^2 - \frac{1}{2}d^2 - \frac{1}{2}e^2 \\ &= de, \end{aligned}$$

by Proposition 2.9.4. Therefore, the number of common roots of f and g in $\mathbb{C}^2$ is less than or equal to de by Theorem 2.9.7.

2.10 Classical resultants

Resultant is a natural notion in elimination theory dealing with the problems of eliminating some variables from a system of polynomial equations. As a toy example, we consider the following system of quadratic equations:

$$\begin{aligned} F(x) &= ax^2 + bx + c = 0, \\ G(x) &= dx^2 + ex + f = 0, \end{aligned}$$

where a, b, c, d, e, f are numbers in $\mathbb{C}$ and $a \neq 0$, $d \neq 0$. By a direct calculation, we can get rid of the variable x, then we obtain

$$a^2f^2 + c^2d^2 + ace^2 + b^2df - abef - bcde - 2cafd = 0.$$

As we will see, this polynomial is called the resultant of F and G. We note that the resultant of F and G vanishes if and only if F and G have a common zero in $\mathbb{C}$. Keeping in mind this example, let us consider the more general cases.

Let $\mathbb{F}$ be a field. $f = \sum_{i=0}^{m} a_i z^i$ and $g = \sum_{i=0}^{n} b_i z^i$ are polynomials in the polynomial ring $\mathbb{F}[z]$ of degree m and n respectively. Suppose f and g have a nontrivial common factor. Then it is easy to see that there are u and v in $\mathbb{F}[z]$ such that the degree of u (resp. v) is less than n (resp. m)

and $uf + vg = 0$. It implies that the following linear map of $\mathbb{F}$-vector spaces

$$\begin{array}{ccc} \mathbb{F}[z]_{n-1} \times \mathbb{F}[z]_{m-1} & \longrightarrow & \mathbb{F}[z]_{m+n-1} \\ (u, v) & \mapsto & uf + vg \end{array}$$

is not surjective, where $\mathbb{F}[z]_d$ denotes the set of all polynomials in z of degree less than or equal to d. The matrix of this linear map with respect to the monomial basis is

$$\begin{pmatrix} a_m & a_{m-1} & \cdots & a_0 & 0 & \cdots & 0 \\ 0 & a_m & a_{m-1} & \cdots & a_0 & \cdots & 0 \\ \vdots & & \ddots & & & \ddots & \vdots \\ 0 & \cdots & 0 & a_m & a_{m-1} & \cdots & a_0 \\ b_n & b_{n-1} & \cdots & b_0 & 0 & \cdots & 0 \\ 0 & b_n & b_{n-1} & \cdots & b_0 & \cdots & 0 \\ \vdots & & \ddots & & & \ddots & \vdots \\ 0 & \cdots & 0 & b_n & b_{n-1} & \cdots & b_0 \end{pmatrix}.$$

We call this the Sylvester matrix of f and g, denoted by $\mathrm{Syl}(f, g)$. Since this matrix does not have full rank, its determinant should be zero. Conversely, if the determinant of the Sylvester matrix of f and g is zero, we can easily to see that f and g have a common factor.

Definition 2.10.1. The resultant $\mathrm{Res}(f, g)$ of f and g is defined by the determinant of the Sylvester matrix $\mathrm{Syl}(f, g)$.

We thus summarize as follows.

Theorem 2.10.2. *Let f and g be polynomials in $\mathbb{F}[z]$. Then f and g have a nontrivial common factor if and only if the resultant $\mathrm{Res}(f, g) = 0$.*

We assume $\mathrm{Res}(f, g) \neq 0$ and consider the equation $uf + vg = 1$, where $u = \sum_{i=0}^{n-1} c_i z^i$, $v = \sum_{i=0}^{m-1} d_i z^i$. This is equivalent to the system of linear equations

$$\mathrm{Syl}(f,g)\cdot\begin{pmatrix} c_0 \\ \vdots \\ c_{n-1} \\ d_0 \\ \vdots \\ d_{m-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ \vdots \\ 0 \\ 1 \end{pmatrix}.$$

By Cramer's rule in linear algebra, we know that

$$c_i = \frac{C_i}{\mathrm{Res}(f,g)} \quad \text{and} \quad d_j = \frac{D_j}{\mathrm{Res}(f,g)},$$

where both C_i and D_j are integer polynomials in the coefficients of f and g. Substituting these into u and v, we obtain the following.

Theorem 2.10.3. *There exist nonzero polynomials* $\tilde{u}$ *and* $\tilde{v}$ *such that* $\tilde{u}f + \tilde{v}g = \mathrm{Res}(f,g)$.

We note that all the $\tilde{u}$, $\tilde{v}$, f and g in Theorem 2.10.3 are polynomials in the variable z, but the resultant $\mathrm{Res}(f,g)$ is not, which depends only on the coefficients of f and g. In this sense, the resultant can be thought of as an outcome by eliminating the variable z in the polynomials f and g.

Now, let us consider the two variable case. Let P and Q be polynomials in $\mathbb{F}[z,w]$ of degree m and n respectively. Then we can write

$$\begin{aligned} P(z,w) &= a_0(z)w^m + a_1(z)w^{m-1} + \cdots + a_m(z), \\ Q(z,w) &= b_0(z)w^n + b_1(z)w^{n-1} + \cdots + b_n(z), \end{aligned}$$

where $a_i(z)$ and $b_j(z)$ are polynomials in z of degree at most i and j respectively. If we think of these polynomials as polynomials in w with coefficients in the function field $\mathbb{F}(z)$, we can define the resultant $\mathrm{Res}_w(P,Q)$ of P and Q in the same way as in the one variable case. Since the coefficients of P and Q are polynomials in z, so is the resultant $\mathrm{Res}_w(P,Q)$. We obtain the following by the same argument as in the one variable case.

Theorem 2.10.4. *Two polynomials* P *and* Q *in* $\mathbb{F}[z, w]$ *have a nontrivial common factor if and only if the resultant* $\mathrm{Res}_w(P, Q)$ *is identically zero. Furthermore, there exist nonzero polynomials* R *and* S *in* $\mathbb{F}[z, w]$ *such that* $RP + SQ = \mathrm{Res}_w(P, Q)$

Note that all the P, Q, R and S in Theorem 2.10.4 are polynomials in z and w, but $\mathrm{Res}_w(P, Q)$ is a polynomial in only one variable z.

In fact, the notion of resultant can be far more generalized. For instance, we can not only deal with the case where several polynomials with several variables, but also the case where a sparse system of polynomials, i.e. a set of polynomials whose monomial terms belongs to a given set of monomials. See [GKZ08] for more details.

2.11 Permanents

Definition 2.11.1. Let $\Sigma = [\sigma_{i,j}]$ be an $n \times n$ square matrix. The permanent of the matrix Σ is defined by

$$\sum_{\lambda \in S_n} \sigma_{1,\lambda(1)} \sigma_{2,\lambda(2)} \cdots \sigma_{n,\lambda(n)}, \tag{2.12}$$

where S_n denotes the set of all permutations of the set $\{1, 2, \cdots, n\}$. We denote the permanent of Σ by $\mathrm{per}(\Sigma)$.

Note that the definition of permanent is almost the same as that of determinant. The only difference is that there are no signatures of permutations in the definition of permanent. Unlike determinant, however, permanent does not even have the multiplicative property, i.e.

$$\mathrm{per}(AB) \neq \mathrm{per}(A) \cdot \mathrm{per}(B).$$

On the other hand, permanent has a useful formula for addition.

Proposition 2.11.2. *[Min84, Chapter 2, Theorem 1.4] Let* A *and* B *be* $n \times n$

square matrices. Then the following formula holds:

$$\mathrm{per}(A+B)=\sum_{i=0}^{n}\sum_{\substack{S,T\in[n]\\|S|=|T|=i}}\mathrm{per}(A[S|T])\mathrm{per}(B(S|T)),$$

where $A[S|T]$ *is the submatrix of* A *consisting of rows indexed by* S *and columns indexed by* T*, and* $B(S|T)$ *is the submatrix of* B *deleting rows indexed by* S *and columns indexed by* T*. If* $|S|=|T|=0$ *(respectively* $|S|=|T|=n$*), we set* $\mathrm{per}(A[S|T])=1$ *(respectively* $\mathrm{per}(B(S|T))=1$*).*

The notion of permanent naturally arises from various combinatorial situations [GK87, DLMV88, McC04]. For instance, if an $n\times n$ square matrix D is the matrix whose diagonal entries are 0 and whose other entries are 1, then its permanent $\mathrm{per}(D)$ is nothing but the number of derangements, i.e. permutations with no fixed points.

From the definition of permanent, we wonder if the permanent is closely related to the determinant. The problem of expressing a permanent of a matrix in terms of determinants of other matrices or more generally, the problem comparing the complexity of permanent to that of determinant are major problems in theoretical computer science. See the Agrawal's ICM talk [Agr06] and the references therein for more details.

Chapter 3

Quantum Separability Problem

The fundamental question in the field of quantum entanglement is to determine whether a given state is entangled or not, which is called the quantum separability problem. For the case of pure states, it is easy to determine the separability. However, for the case of mixed states, the separability problem of a quantum states is extremely hard to solve in general setting, it is actually known to be an **NP**-hard problem even for the bipartite case [Gur03, Gha10].

3.1 Separability for pure states

We recall that a pure state is, by definition, a vector in a Hilbert space. A bipartite pure state $|\psi\rangle$ in a composite quantum system $\mathcal{H}_1 \otimes \mathcal{H}_2$ is called separable if it can be written as a tensor product of two states, each of which belongs to the Hilbert space of the corresponding subsystems, i.e.

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle,$$

where $|\psi_1\rangle \in \mathcal{H}_1$, $|\psi_2\rangle \in \mathcal{H}_2$. In general, any state $|\psi\rangle$ in $\mathcal{H}_1 \otimes \mathcal{H}_2$ is written as

$$|\psi\rangle = \sum_{i,j} a_{ij} |\psi_1^{(i)}\rangle \otimes |\psi_2^{(j)}\rangle,$$

where $|\psi_1^{(i)}\rangle$ and $|\psi_2^{(j)}\rangle$ are bases of $\mathcal{H}_1$ and $\mathcal{H}_2$ respectively. We can easily check that the state $|\psi\rangle$ is separable if and only if the matrix (a_{ij}) has rank one. In practice, by the singular value decomposition in linear algebra, the state $|\psi\rangle$ can be expressed as

$$|\psi\rangle = \sum_{i=1}^{\min(\dim \mathcal{H}_1, \dim \mathcal{H}_2)} \lambda_i |e_1^{(i)}\rangle \otimes |e_2^{(i)}\rangle, \tag{3.1}$$

where $|e_1^{(i)}\rangle$ and $|e_2^{(i)}\rangle$ are orthonormal sets in $\mathcal{H}_1$ and $\mathcal{H}_2$ respectively and λ_i are nonnegative real numbers. This is called the Schmidt decomposition and λ_i the Schmidt coefficients. The number of nonzero λ_i is called the Schmidt rank of $|\psi\rangle$. The state $|\psi\rangle$ is separable if and only if the Schmidt rank of $|\psi\rangle$ is one. In order to decompose the state ρ into the Schmidt form (3.1), we introduce the following.

Definition 3.1.1. Let ρ be an operator on $\bigotimes_{i=1}^n \mathcal{H}_i$, i.e. an element in the set of all linear maps from $\bigotimes_{i=1}^n \mathcal{H}_i$ to itself $\mathrm{End}\,(\bigotimes_{i=1}^n \mathcal{H}_i)$. We write the operator ρ as

$$\rho = \sum_k \alpha_k \bigotimes_{i=1}^n |\psi_i^{(k)}\rangle\langle\phi_i^{(k)}|,$$

where $|\psi_i^{(k)}\rangle$ and $\langle\phi_i^{(k)}|$ are elements in each subsystem $\mathcal{H}_i$ and its dual $\mathcal{H}_i^*$ respectively. Let $\mathcal{I}$ be a subset of $\{1, 2, \cdots, n\}$. Then the partial trace $\mathrm{tr}_{\mathcal{I}}$ is defined by

$$\mathrm{tr}_{\mathcal{I}}(\rho) := \sum_k \alpha_k \left(\prod_{i\in\mathcal{I}} \langle\phi_i^{(k)}|\psi_i^{(k)}\rangle \right) \bigotimes_{i\in\{1,\cdots,n\}\setminus\mathcal{I}} |\psi_i^{(k)}\rangle\langle\phi_i^{(k)}|,$$

which is an element in $\mathrm{End}\left(\bigotimes_{i\in\{1,\cdots,n\}\setminus\mathcal{I}} \mathcal{H}_i\right)$. Sometimes $\mathrm{tr}_{\mathcal{I}}(\rho)$ is called the reduced density matrix of the subsystem $\bigotimes_{i\in\{1,\cdots,n\}\setminus\mathcal{I}} \mathcal{H}_i$.

If the state $|\psi\rangle$ has the Schmidt form (3.1), then

$$\mathrm{tr}_1(|\psi\rangle\langle\psi|) = \sum_i \lambda_i^2 |e_2^{(i)}\rangle\langle e_2^{(i)}|$$
$$\mathrm{tr}_2(|\psi\rangle\langle\psi|) = \sum_i \lambda_i^2 |e_1^{(i)}\rangle\langle e_1^{(i)}|$$

We note that $|e_1^{(i)}\rangle$ and $|e_2^{(i)}\rangle$ are nothing but the eigenvectors of $\mathrm{tr}_1(|\psi\rangle\langle\psi|)$ and $\mathrm{tr}_2(|\psi\rangle\langle\psi|)$ respectively, and the Schmidt coefficients are the square roots of the common eigenvalues of $\mathrm{tr}_1(|\psi\rangle\langle\psi|)$ and $\mathrm{tr}_2(|\psi\rangle\langle\psi|)$.

For the case of multipartite pure states, a pure state $|\psi\rangle$ in a composite quantum system $\bigotimes_{i=1}^n \mathcal{H}_i$ is called (fully) separable if it can be written as

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle,$$

where $|\psi_i\rangle \in \mathcal{H}_i$. To check the separability of a given multipartite pure states $|\psi\rangle$, it suffices to compute the reduced density matrices $\mathrm{tr}_i(|\psi\rangle\langle\psi|)$ for every i and check whether they are product states.

Unlike the bipartite case, the state $|\psi\rangle$ does not admit the generalized Schmidt form

$$|\psi\rangle = \sum_{i=1}^m \lambda_i |e_1^{(i)}\rangle \otimes \cdots \otimes |e_n^{(i)}\rangle,$$

where $m = \min(\dim \mathcal{H}_1, \cdots, \dim \mathcal{H}_n)$ and $|e_j^{(i)}\rangle$ are orthonormal sets in $\mathcal{H}_i$ for every j. If a state kp admit the generalized Schmidt form, then it can be easily checked that the partial trace $\mathrm{tr}_i(|\psi\rangle\langle\psi|)$ should be a mixed separable state for every i. However, the state

$$|W\rangle = \frac{1}{\sqrt{3}}(|100\rangle + |010\rangle + |001\rangle)$$

has an entangled two-qubit subsystem, so it does not admit the generalized Schmidt form.

3.2 PPT criterion and positive linear maps

In bipartite case, the most convenient and powerful criterion for separability is the so called PPT criterion by Choi [Cho82] and Peres [Per96]. Let M_1 and M_2 be $m \times m$ and $n \times n$ square matrices over $\mathbb{C}$ respectively. Then the partial transpose $(M_1 \otimes M_2)^\Gamma$ of $M_1 \otimes M_2$ is defined by

$$(M_1 \otimes M_2)^\Gamma := M_1^t \otimes M_2,$$

where M^t is the usual transpose of the matrix M. This definition naturally extends to any element of $\mathfrak{M}_m \otimes \mathfrak{M}_n$ by linearity, where $\mathfrak{M}_n$ is the set of $n \times n$ square matrices over the field of complex numbers $\mathbb{C}$.

To see what the partial transpose of $M_1 \otimes M_2$ is more vividly, we write $M_1 \otimes M_2$ as follows in terms of the entries of the matrices:

$$\begin{pmatrix} a_{11}M_2 & a_{12}M_2 & \cdots & a_{1m}M_2 \\ a_{21}M_2 & a_{22}M_2 & \cdots & a_{2m}M_2 \\ \vdots & \vdots & \ddots & \cdots \\ a_{m1}M_2 & a_{m2}M_2 & \cdots & a_{mm}M_2 \end{pmatrix},$$

where $M_1 = (a_{ij})$. Then the partial transpose $(M_1 \otimes M_2)^\Gamma$ of $M_1 \otimes M_2$ is

$$\begin{pmatrix} a_{11}M_2 & a_{21}M_2 & \cdots & a_{m1}M_2 \\ a_{12}M_2 & a_{22}M_2 & \cdots & a_{m2}M_2 \\ \vdots & \vdots & \ddots & \cdots \\ a_{1m}M_2 & a_{2m}M_2 & \cdots & a_{mm}M_2 \end{pmatrix}.$$

Note that this is nothing but the usual transpose of the $mn \times mn$ matrix $M_1 \otimes M_2$ as the $m \times m$ block matrix whose entries are $n \times n$ matrices. Sometimes this is called a blockwise transpose.

Definition 3.2.1. Let ρ be a state on a finite-dimensional Hilbert space $\mathbb{C}^m \otimes \mathbb{C}^n$. Then we call the state ρ is a PPT (positive partial transpose) state if its partial transpose ρ^Γ of ρ is positive semi-definite when we consider the state ρ as an element in $\mathfrak{M}_m \otimes \mathfrak{M}_n$.

Theorem 3.2.2. *(PPT criterion) Let ρ be a state on a finite dimensional bipartite quantum system. If the state ρ is separable, then it is a PPT state.*

Proof. Let

$$\rho = \sum_k p_k |\psi_1^{(k)}\rangle \otimes |\psi_2^{(k)}\rangle\langle\psi_1^{(k)}| \otimes \langle\psi_2^{(k)}|.$$

Then its partial transpose ρ^Γ is

$$\begin{aligned}
\rho^\Gamma &= \sum_k p_k \left(|\psi_1^{(k)}\rangle \otimes |\psi_2^{(k)}\rangle\langle\psi_1^{(k)}| \otimes \langle\psi_2^{(k)}|\right)^\Gamma \\
&= \sum_k p_k \left(|\psi_1^{(k)}\rangle\langle\psi_1^{(k)}| \otimes |\psi_2^{(k)}\rangle\langle\psi_2^{(k)}|\right)^\Gamma \\
&= \sum_k p_k \left(|\psi_1^{(k)}\rangle\langle\psi_1^{(k)}|\right)^t \otimes |\psi_2^{(k)}\rangle\langle\psi_2^{(k)}| \\
&= \sum_k p_k |\overline{\psi_1^{(k)}}\rangle\langle\overline{\psi_1^{(k)}}| \otimes |\psi_2^{(k)}\rangle\langle\psi_2^{(k)}|,
\end{aligned}$$

where $|\overline{\psi}\rangle$ is the complex conjugate of $|\psi\rangle$. This implies that ρ^Γ is positive semi-definite. □

As you can see here, the proof of the PPT criterion is surprisingly simple, but the PPT criterion is known to be stronger than Rényi entropy of order α for any $\alpha \in [0, \infty]$ [VW02].

The PPT criterion is sufficient to verify separability only for the $2 \otimes 2$ and the $2 \otimes 3$ cases [HHH96] and there are examples of entangled states with positive partial transpose (PPTES) in the $3 \otimes 3$ and the $2 \otimes 4$ cases [Hor97, Wor76]. The first example of PPT entangled states in $3 \otimes 3$ case appeared in [Cho82] in a slight different language.

Historically, operator algebraists in the field of mathematics have been intensively studied various positive linear maps since the middle of the 20th century, the version of the PPT criterion in terms of positive linear maps was first found by Choi [Cho82], one of operator algebraists.

The relation between the two sides is realized by the duality between the set of all linear maps from $\mathfrak{M}_m$ to $\mathfrak{M}_n$, denoted by $\mathcal{L}(\mathfrak{M}_m, \mathfrak{M}_n)$ and

$\mathfrak{M}_m \otimes \mathfrak{M}_n$. It corresponds the set of all positive linear maps (resp. decomposable maps) to that of separable states (resp. PPT states). Hence, the condition that any PPT states are separable for the case $2 \otimes 2$ or $2 \otimes 3$ is equivalent that there are no indecomposable positive linear maps in the space of linear maps $\mathcal{L}(\mathfrak{M}_2, \mathfrak{M}_2)$ or $\mathcal{L}(\mathfrak{M}_2, \mathfrak{M}_3)$. Moreover, examples of PPT entangled states corresponds to indecomposable positive linear maps. See [Kye12] for more details. The works of Choi [Cho82] and Woronowicz [Wor76] were realized in this sense. From the view of quantum information or mathematics itself, the indecomposable positive linear maps are intensively studied by several mathematicians such as Osaka [Osa91, Osa93], Kye and Ha [HKP03, HK04], and so on.

Example 3.2.3. Let ρ_1 and ρ_2 be states on a composite quantum system $\mathbb{C}^2 \otimes \mathbb{C}^2$ defined as follows:

$$\rho_1 = \frac{1}{4}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}, \quad \rho_2 = \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & -1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Since

$$\rho_1^\Gamma = \frac{1}{4}\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}, \quad \rho_2^\Gamma = \frac{1}{2}\begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix},$$

ρ_1^Γ is positive semi-definite, but ρ_2^Γ is not because its determinant is negative. It means that the state ρ_1 is a PPT state, but the state ρ_2 is not. By the PPT criterion, ρ_2 is entangled. In fact,

$$\rho_1 = \frac{1}{2} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} + \frac{1}{2} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix},$$

so ρ_1 is separable.

In multipartite case, we can directly generalize the PPT criterion in The-

orem 3.2.2. Let M_j be $d_j \times d_j$ square matrices over $\mathbb{C}$. For a given subset S of $\{1, 2, \cdots, n\}$, we define the partial transpose $\left(\bigotimes_{j=1}^{n} M_j\right)^{T(S)}$ of $\bigotimes_{j=1}^{n} M_j$ by

$$(M_1 \otimes M_2 \otimes \cdots \otimes M_n)^{T(S)} := M_1' \otimes M_2' \otimes \cdots \otimes M_n', \quad \text{with } M_j' = \begin{cases} M_j^t, & j \in S, \\ M_j, & j \notin S, \end{cases}$$

and extend the map to the whole $\bigotimes_{j=1}^{n} \mathfrak{M}_{d_j}$ by linearity, where M^t denotes the transpose of the matrix M.

Definition 3.2.4. Let ρ be a state on a finite dimensional multipartite quantum system $\mathcal{H} = \bigotimes_{i=1}^{n} \mathcal{H}_i$. We say that a state ρ is of PPT if its partial transpose $\rho^{T(S)}$ is positive for every subset S of $\{1, 2, \cdots, n\}$.

It is easily checked that every separable state is of PPT, as it was observed for the bi-partite case $n = 2$. We note that $\rho^{T(S)}$ is positive if and only if $\rho^{T(S^c)}$ is positive, where S^c is the complement of S in $\{1, 2, \cdots, n\}$. Therefore, it is enough to check the positivity of 2^{n-1} matrices among 2^n matrices, to confirm the PPT property of a given n-partite state.

3.3 Range criterion

Since the PPT condition is not sufficient for a state to be separable except for a few cases, we need to find another criterion to determine if a given PPT state is separable or not. Horodecki [Hor97] formulated a criterion for this purpose in bipartite case by looking at the ranges of the state and its partial transpose, which is called the range criterion.

Theorem 3.3.1. *(The range criterion) Let ρ be a PPT state on a finite dimensional bipartite quantum system. If the state ρ is separable, then there exists a collection $\left\{|\psi_1^{(k)}\rangle \otimes |\psi_2^{(k)}\rangle\right\}$ of product vectors such that $\left\{|\psi_1^{(k)}\rangle \otimes |\psi_2^{(k)}\rangle\right\}$ span the range $\mathcal{R}(\rho)$ of ρ and $\left\{\overline{|\psi_1^{(k)}\rangle} \otimes |\psi_2^{(k)}\rangle\right\}$ the range $\mathcal{R}(\rho^\Gamma)$ of ρ^Γ.*

Proof. Let

$$\rho = \sum_k p_k |\psi_1^{(k)}\rangle \otimes |\psi_2^{(k)}\rangle\langle\psi_1^{(k)}| \otimes \langle\psi_2^{(k)}|.$$

It is obvious that the range of ρ is contained in the vector space spanned by $\left\{|\psi_1^{(k)}\rangle \otimes |\psi_2^{(k)}\rangle\right\}$. Conversely, when we take any vector $|\psi_1^{(k)}\rangle \otimes |\psi_2^{(k)}\rangle$, we need to show it is contained in the range of ρ. Without loss of generality, we let $k = 1$. Then we can write ρ as

$$\rho = p_1 |\psi_1^{(1)}\rangle \otimes |\psi_2^{(1)}\rangle\langle\psi_1^{(1)}| \otimes \langle\psi_2^{(1)}| + \tilde{\rho},$$

where $\tilde{\rho} = \sum_{k\neq 1} p_k |\psi_1^{(k)}\rangle \otimes |\psi_2^{(k)}\rangle\langle\psi_1^{(k)}| \otimes \langle\psi_2^{(k)}|$. If $|\psi_1^{(1)}\rangle \otimes |\psi_2^{(1)}\rangle$ is contained in the kernel of $\tilde{\rho}$, we have done. If not, i.e. $\text{span}\left\{|\psi_1^{(1)}\rangle \otimes |\psi_2^{(1)}\rangle\right\} \nsubseteq \text{Ker}\,\tilde{\rho}$, then $\mathcal{R}(\tilde{\rho}) = (\text{Ker}\,\tilde{\rho})^\perp \nsubseteq \text{span}\left\{|\psi_1^{(1)}\rangle \otimes |\psi_2^{(1)}\rangle\right\}^\perp$ since $\tilde{\rho}$ is Hermitian. This implies that $\mathcal{R}(\tilde{\rho}) \cap \text{span}\left\{|\psi_1^{(1)}\rangle \otimes |\psi_2^{(1)}\rangle\right\} \neq \{0\}$, i.e. $|\psi_1^{(1)}\rangle \otimes |\psi_2^{(1)}\rangle \in \mathcal{R}(\tilde{\rho})$. Hence it is also clear that $|\psi_1^{(1)}\rangle \otimes |\psi_2^{(1)}\rangle$ belongs to the range of ρ. By the proof of Theorem 3.2.2, we have known that

$$\rho^\Gamma = \sum_k p_k \overline{|\psi_1^{(k)}\rangle}\overline{\langle\psi_1^{(k)}|} \otimes |\psi_2^{(k)}\rangle\langle\psi_2^{(k)}|,$$

so we can also obtain $\mathcal{R}(\rho^\Gamma) = \text{span}\left\{\overline{|\psi_1^{(k)}\rangle} \otimes |\psi_2^{(k)}\rangle\right\}$ by performing the similar process in the case of ρ. □

Example 3.3.2. [Kye12] We consider the state ρ on $\mathbb{C}^3 \otimes \mathbb{C}^3$ defined by

$$\rho = \frac{2}{21}\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 2 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{2} & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & \frac{1}{2} & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & \frac{1}{2} & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}. \tag{3.2}$$

We can easily check that ρ is a PPT state. Moreover, the range of ρ is the 4-dimensional space spanned by

$$|00\rangle + |11\rangle + |22\rangle, \quad \sqrt{2}|01\rangle + \frac{1}{\sqrt{2}}|10\rangle,$$
$$\sqrt{2}|12\rangle + \frac{1}{\sqrt{2}}|21\rangle, \quad \sqrt{2}|20\rangle + \frac{1}{\sqrt{2}}|02\rangle,$$

where $|0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, $|1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$, $|2\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$.

It is easy to see that the corresponding 4-dimensional subspace of $M_{3\times 3}$ spanned by

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & \sqrt{2} & 0 \\ \frac{1}{\sqrt{2}} & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & \sqrt{2} \\ 0 & \frac{1}{\sqrt{2}} & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & \frac{1}{\sqrt{2}} \\ 0 & 0 & 0 \\ \sqrt{2} & 0 & 0 \end{pmatrix}$$

has no rank one matrices, which implies that the matrix in (3.2) is entangled. This is the first example of $3 \otimes 3$ PPTES given by Choi [Cho82].

Like the PPT criterion, we can directly generalize the range criterion in the multipartite cases. For a subset S of $\{1, 2, \cdots, n\}$ and a product vector $|\psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$ in a finite dimensional Hilbert space $\mathcal{H} = \bigotimes_{i=1}^{n} \mathcal{H}_i$, we define by the partial transpose $|\psi\rangle^{\Gamma(S)}$ of $|\psi\rangle$ up to constant by

$$(|\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle)^{\Gamma(S)} := |\phi_1\rangle \otimes \cdots \otimes |\phi_n\rangle, \quad \text{with } |\phi_j\rangle = \begin{cases} |\bar{\psi}_j\rangle, & j \in S, \\ |\psi_j\rangle, & j \notin S. \end{cases} \tag{3.3}$$

Theorem 3.3.3 (Range Criterion for multipartite cases)**.** *If a given PPT state ρ on a composite quantum system $\mathcal{H} = \bigotimes_{i=1}^{n} \mathcal{H}_i$ is separable then there exists a collection $\{|\psi\rangle : |\psi\rangle \in \Psi\}$ of product vectors with the following property: The range of $\rho^{T(S)}$ is the span of the product vectors $\{|\psi\rangle^{\Gamma(S)} : |\psi\rangle \in \Psi\}$ for each subset S of $\{1, 2, \cdots, n\}$.*

Therefore, the following questions naturally arise.

Question 3.3.4. For given a PPT state ρ on a composite quantum system $\mathcal{H} = \bigotimes_{i=1}^{n} \mathcal{H}_i$, is there a nonzero product vector $|\psi\rangle$ such that $|\psi\rangle^{\Gamma(S)}$ belong to the ranges $\mathcal{R}(\rho^{T(S)})$ for every subset S of $\{1, 2, \cdots, n\}$?

Question 3.3.5. If exist, how many different product vectors in $\mathcal{H} = \bigotimes_{i=1}^{n} \mathcal{H}_i$ up to constant are there such that $|\psi\rangle^{\Gamma(S)}$ belong to the ranges $\mathcal{R}(\rho^{T(S)})$ for every subset S of $\{1, 2, \cdots, n\}$?

Chapter 4

Algebraic Criterion for Separability

By the range criterion, if a PPT state ρ on a composite quantum system $\mathcal{H} = \bigotimes_{i=1}^{n} \mathcal{H}_i$ is separable, then there exists a collection $\left\{ |\psi^{(i)}\rangle \right\}_{i\in I}$ of product vectors with the following property:

For every subset S *of* $\{1, 2, \cdots, n\}$*, the range of* $\rho^{\Gamma(S)}$ *is spanned by the set of the product vectors* $\left\{ \left(|\psi\rangle^{(i)}\right)^{\Gamma(S)} \right\}_{i\in I}$.

Hence, the existence of a nonzero product vector $|\psi\rangle$ such that $|\psi\rangle^{\Gamma(S)}$ belongs to the range of $\rho^{\Gamma(S)}$ for every subset S of $\{1, 2, \cdots, n\}$ is a minimum necessary condition for ρ to be separable.

Suppose that we are given finite sequences $\{S_1, S_2, \cdots S_r\}$ of subsets of $\{1, 2, \cdots, n\}$ and $\{D_1, D_2 \cdots, D_r\}$ of subspaces of $\mathcal{H}$. In this chapter, we investigate the conditions for which there is a nonzero product vector $|\psi\rangle$ satisfying the conditions

$$|\psi\rangle^{\Gamma(S_i)} \in D_i, \qquad i = 1, 2, \cdots, r. \tag{4.1}$$

These observations give us an algebraic criterion to determine whether Question 3.3.4 has an affirmative answer.

4.1 Algebraic criterion for bipartite cases

Note that the condition

$$|\psi_1\rangle \otimes |\psi_2\rangle \in D, \qquad |\overline{\psi_1}\rangle \otimes |\psi_2\rangle \in E. \tag{4.2}$$

is nothing but the problem of solving a system of polynomial equations [HLVC00, KCKL00]. In the next chapter, we will deal with the equations directly, so see Section 5.1 for more details. Let $\dim D^{\perp} = k$ and $\dim E^{\perp} = \ell$. Since the number of equations and that of variables are $k + \ell$ and $m + n - 2$ respectively, it is natural to divide the problem into the following three cases:

- Over-determined case: $k + \ell > m + n - 2$
- Critical case : $k + \ell = m + n - 2$
- Under-determined case : $k + \ell < m + n - 2$

Throughout this thesis, We say that a property holds for *generic* subspaces D in $\mathbb{C}^n$ with $\dim D^{\perp} = k$ if there is a subset $\mathfrak{U}$ of the Grassmann variety $\mathrm{Gr}(k, d)$ whose complement is of measure zero such that the property holds for all $D \in \mathfrak{U}$. We remark that the term 'generic' could be changed to be 'almost all' or 'almost surely' in the sense of [RW09, WS08].

Theorem 4.1.1 (Algebraic Criterion)**.** *[KKL11] Let D and E be subspaces of $\mathbb{C}^m \otimes \mathbb{C}^n$ with $\dim D^{\perp} = k, \dim E^{\perp} = \ell$.*

(1) If $k+\ell > m+n-2$, then there is no nonzero product vector $|\psi_1\rangle \otimes |\psi_2\rangle \in D$ with $|\overline{\psi_1}\rangle \otimes |\psi_2\rangle \in E$ for generic choices of D and E.

(2) If $k+\ell = m+n-2$ and $\sum_{r+s=m-1}(-1)^r \binom{k}{r}\binom{\ell}{s} \neq 0$, there exists a nonzero product vector $|\psi_1\rangle \otimes |\psi_2\rangle \in D$ with $|\overline{\psi_1}\rangle \otimes |\psi_2\rangle \in E$.

(3) If $k+\ell < m+n-2$, there are infinitely many product vectors $|\psi_1\rangle \otimes |\psi_2\rangle \in D$ with $|\overline{\psi_1}\rangle \otimes |\psi_2\rangle \in E$.

Proof. Let us consider the following diagram:

$$\begin{array}{ccc} \mathbb{P}^{m-1} \times \mathbb{P}^{n-1} & \xhookrightarrow{\quad i \quad} & \mathbb{P}^{mn-1} \\ \phi \downarrow & & \\ \mathbb{P}^{m-1} \times \mathbb{P}^{n-1} & \xhookrightarrow{\quad i \quad} & \mathbb{P}^{mn-1} \end{array}$$

,where $\mathfrak{i}$ is the Segre embedding and ϕ is a diffeomorphism given by $(x, y) \mapsto (\bar{x}, y)$. We notice that $\phi\left(\mathfrak{i}^{-1}(\mathbb{P}D)\right) \cap \mathfrak{i}^{-1}(\mathbb{P}E)$ is nothing but

$$\phi\left(\mathfrak{i}^{-1}(\mathbb{P}D)\right) \cap \mathfrak{i}^{-1}(\mathbb{P}E) = \{(\bar{x}, y) \in \mathbb{P}^{m-1} \times \mathbb{P}^{n-1} | \, x \otimes y \in D, \bar{x} \otimes y \in E\}.$$

Therefore, we have to estimate the size of the set described above. Now, we use the homological method in intersection theory. In the cohomology ring $H^*(\mathbb{P}^{m-1} \times \mathbb{P}^{n-1}, \mathbb{Z}) \cong \mathbb{Z}[\alpha, \beta]/\langle \alpha^m, \beta^n \rangle$, we can readily check that the class $(-\alpha+\beta)^k(\alpha+\beta)^\ell$ is the Poincaré dual of small perturbation of $\phi\left(\mathfrak{i}^{-1}(\mathbb{P}D)\right) \cap \mathfrak{i}^{-1}(\mathbb{P}E)$. If the set $\phi\left(\mathfrak{i}^{-1}(\mathbb{P}D)\right) \cap \mathfrak{i}^{-1}(\mathbb{P}E)$ is empty, then so is its small perturbation, hence the class $(-\alpha+\beta)^k(\alpha+\beta)^\ell$ must be zero. This implies that nonvanishing of the class $(-\alpha+\beta)^k(\alpha+\beta)^l$ is a sufficient condition that there is a nonzero product vector $|\psi_1\rangle \otimes |\psi_2\rangle \in D$ with $|\overline{\psi_1}\rangle \otimes |\psi_2\rangle \in E$.

First, we prove the over-determined case $k+\ell > m+n-2$. For a generic choice of D, we consider the set of E's for which there exists a nonzero product vector $|\psi_1\rangle \otimes |\psi_2\rangle \in D$ with $|\overline{\psi_1}\rangle \otimes |\psi_2\rangle \in E$. Note that it is a proper subset in $\mathrm{Gr}(l, mn)$ of real dimension $\dim_{\mathbb{R}} \mathrm{Gr}(\ell, mn) - 2(k+\ell-m-n+2))$, so there is no nonzero product vector $|\psi_1\rangle \otimes |\psi_2\rangle \in D$ with $|\overline{\psi_1}\rangle \otimes |\psi_2\rangle \in E$ for generic choices of D and E.

If $k + \ell = m + n - 2$, then the class $(-\alpha + \beta)^k(\alpha + \beta)^\ell$ is a single term $\sum_{r+s=m-1}(-1)^r\binom{k}{r}\binom{\ell}{s}\alpha^k\beta^l$ in the cohomology ring $H^*(\mathbb{P}^{m-1} \times \mathbb{P}^{n-1}, \mathbb{Z})$, so there is a nonzero product vector $|\psi_1\rangle \otimes |\psi_2\rangle \in D$ with $|\overline{\psi_1}\rangle \otimes |\psi_2\rangle \in E$ if the coefficient $\sum_{r+s=m-1}(-1)^r\binom{k}{r}\binom{\ell}{s}$ of $\alpha^k\beta^\ell$ is not zero.

If $k+\ell < m+n-2$, then $(-\alpha+\beta)^k(\alpha+\beta)^\ell$ must be a positive dimensional class because we can easily check that the consecutive coefficients of

the polynomial $(-1+t)^k(1+t)^\ell$ can not be simultaneously zero. Thus the cardinality of the set $\phi\left(i^{-1}(\mathbb{P}D)\right) \cap i^{-1}(\mathbb{P}E)$ is infinite. □

The results in the over-determined case (1) and the under-determined case (3) are seemed to be natural and easy to prove it at first glance, however it has subtlety in general because the problem deals with a system of polynomial equations not in only complex variables, but in complex variables and their complex conjugates. This is the main reason why we use inevitably the homological methods in intersection theory instead of easier theorems such as Bezout's theorem. From Theorem 4.1.1, we get the following.

Corollary 4.1.2. *Let ρ be a PPT state on a composite quantum system $\mathbb{C}^m \otimes \mathbb{C}^n$. Let $\dim \mathcal{R}(\rho)^\perp = k$ and $\dim \mathcal{R}(\rho^\Gamma)^\perp = \ell$. Then the following holds.*

(1) If $k+\ell > m+n-2$, then ρ is almost surely entangled.

(2) If $k+\ell = m+n-2$ and $\sum_{r+s=m-1}(-1)^r\binom{k}{r}\binom{\ell}{s} = 0$, then ρ is entangled.

We note that there is not always a nonzero product vector $|\psi_1\rangle \otimes |\psi_2\rangle$ satisfying (4.2) even for the critical case $k+\ell = m+n-2$. The algebraic condition

$$\sum_{r+s=m-1} (-1)^r \binom{k}{r}\binom{l}{s} = 0 \tag{4.3}$$

may happen for the following cases:

(i) When $m = 2$, the relation (4.3) holds if and only if $n = 2k$ and $\ell = k$.

(ii) When $m = 3$, the relation (4.3) holds if and only if

$$n = r(r+2), \quad k = \binom{r+1}{2} \quad \text{and} \quad \ell = \binom{r+2}{2}$$

for a positive integer r.

(iii) When $m = n$, the relation (4.3) holds if and only if k and ℓ are odd.

(iv) When $k = \ell$, the relation (4.3) holds if and only if m and n are even.

Example 4.1.3. [KKL11] Let $\{|0\rangle, |1\rangle\}$ be an orthonormal basis for $\mathbb{C}^2$. Let $|\beta_1\rangle = |00\rangle + |11\rangle$ and $|\beta_2\rangle = |01\rangle - |10\rangle$. For two nonzero vectors $|\psi_1\rangle, |\psi_2\rangle$ in $\mathbb{C}^2$, we have

$$\langle \psi_1, \bar{\psi}_2 | \beta_1 \rangle = \langle \psi_1 | 0 \rangle \langle \bar{\psi}_2 | 0 \rangle + \langle \psi_1 | 1 \rangle \langle \bar{\psi}_2 | 1 \rangle = \langle \psi_1 | \psi_2 \rangle.$$

Therefore, we see that the equation $\langle \psi_1, \bar{\psi}_2 | \beta_1 \rangle = 0$ is equivalent to the orthogonality of $|\psi_1\rangle$ and $|\psi_2\rangle$. Similarly, the equation $\langle \psi_1, \psi_2 | \beta_2 \rangle = 0$ is equivalent to saying that $|\psi_1\rangle$ and $|\psi_2\rangle$ are parallel. If we put $D_1 = |\beta_1\rangle^\perp$ and $D_2 = |\beta_2\rangle^\perp$ then the system of equations

$$\begin{aligned} |\psi_1, \bar{\psi}_2\rangle &\in D_1 \\ |\psi_1, \psi_2\rangle &\in D_2 \end{aligned} \tag{4.4}$$

has no nonzero solution even though this is the critical case.

4.2 Algebraic criterion for multipartite cases

Unlike the bipartite cases, there are few results on the separability problem on multipartite mixed states. In this section, we generalize the homological method used in Theorem 4.1.1 to the multipartite settings. Recall that we have to investigate the system of equations

$$|\psi\rangle^{\Gamma(S_i)} \in D_i, \qquad i = 1, 2, \cdots, r, \tag{4.5}$$

with variables $|\psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle$ in the Segre variety $Seg(\mathbb{P}^{d_1-1} \times \cdots \times \mathbb{P}^{d_n-1}) \subset \prod_{j=1}^{n} \mathbb{P}^{d_j-1}$.

To do this, it is convenient to define the $r \times n$ matrix $\Sigma = [\sigma_{ij}]$ with entries

$$\sigma_{ij} = \begin{cases} -1, & j \in S_i, \\ +1, & j \notin S_i, \end{cases}$$

which will be called the associated matrix of the sequence $\{S_1, S_2, \cdots S_r\}$. We note that the number N_U of unknowns of the system of equations (4.5) is given by

$$N_U = \sum_{j=1}^{n} (d_j - 1),$$

which is the dimension of the variety $Seg(\mathbb{CP}^{d_1-1} \times \cdots \times \mathbb{CP}^{d_n-1})$. On the other hand, the number N_E of algebraic equations in (4.5) is just $N_E = \sum_{i=1}^{r} \dim D_i^{\perp}$. Now, we are ready to state the main result of this section:

Theorem 4.2.1. *Let $\{S_1, \cdots, S_r\}$ be a sequence of subsets of $[n] := \{1, 2, \cdots, n\}$ with the associated matrix $\Sigma = [\sigma_{ij}]$. Then we have the following:*

(i) If $N_E = \sum_{i=1}^{r} k_i > N_U$, then the system of equations (4.5) has no nonzero solution for generic subspaces D_i of $\mathcal{H}$ with $k_i = \dim D_i^{\perp}$ for $i = 1, 2, \cdots, r$.

(ii) Suppose that $N_E = N_U$, and the coefficient of $\prod_j \alpha_j^{d_j-1}$ is nonzero when we expand the polynomial

$$\prod_{i=1}^{r} (\sigma_{i,1}\alpha_1 + \sigma_{i,2}\alpha_2 + \cdots + \sigma_{i,n}\alpha_n)^{\dim D_i^{\perp}} \tag{4.6}$$

Then the system of equations (4.5) has a nonzero solution.

(iii) If $N_E < N_U$ and the associate matrix Σ has rank r, then the system of equations (4.5) has infinitely many solutions.

The proof of Theorem 4.2.1 is so lengthy, we assign a section to prove it.

4.3 Proof of Theorem 4.2.1

4.3.1 Over-determined case

We recall that a property holds for *generic* subspaces D in $\mathbb{C}^d$ with $\dim D^{\perp} = k$ if there is a subset $\mathfrak{U}$ of the Grassmann variety $Gr(k, d)$ whose complement

is of measure zero such that the property holds for all $D \in \mathfrak{U}$.

Theorem 4.2.1 (i) is a consequence of dimension estimates and the Morse-Sard theorem. Consider the following diagram:

$$\begin{array}{ccc} \prod_{j=1}^{n} \mathbb{P}^{d_j-1} & & \\ \Big\downarrow{\scriptstyle \phi^{\Gamma(S)}} & & \\ \prod_{j=1}^{n} \mathbb{P}^{d_j-1} & \xhookrightarrow{\quad \iota \quad} & \mathbb{P}^{d-1} \end{array} \tag{4.7}$$

where $d = \prod_j d_j$. For $S \subset [n] := \{1, 2, \cdots, n\}$, the map $\phi^{\Gamma(S)}$ is the diffeomorphism which sends $([|\psi_j\rangle])$ to $([|\phi_j\rangle])$, where $|\phi_j\rangle$ is given by

$$|\phi_j\rangle = \begin{cases} |\bar{\psi}_j\rangle, & j \in S, \\ |\psi_j\rangle, & j \notin S, \end{cases}$$

and $[|\psi\rangle] \in \mathbb{P}^{d-1}$ denotes the line spanned by $|\psi\rangle$. The injective map ι is the Segre embedding which sends $([|\psi_j\rangle])$ to $[\otimes_{j=1}^{n}|\psi_j\rangle]$. We want to show that the set

$$\bigcap_{i=1}^{r} \left(\phi^{\Gamma(S_i)}\right)^{-1} \left(\iota^{-1}(\mathbb{P}D_i)\right) = \left\{ ([|\psi_j\rangle]) \in \prod_{j=1}^{n} \mathbb{P}^{d_j-1} \mid \left(\otimes_{j=1}^{n}|\psi_j\rangle\right)^{\Gamma(S_i)} \in D_i \right\} \tag{4.8}$$

is empty for generic choices of D_i.

By Bertini's theorem [Har77, Chapter II, Theorem 8.18], we may choose a generic D_1 such that $\iota^{-1}(\mathbb{P}D_1)$ is a smooth manifold of real dimension $2(N_U - k_1)$. Let $E_1 := \left(\phi^{\Gamma(S_1)}\right)^{-1} \left(\iota^{-1}(\mathbb{P}D_1)\right)$. In order to choose D_2, let us consider the universal bundle $\mathcal{U}_2$ over $\mathrm{Gr}(d, k_2)$ so that we have a diagram:

$$\begin{array}{ccc} \mathbb{P}\mathcal{U}_2 & \hookrightarrow & \mathbb{P}^{d-1} \times \mathrm{Gr}(d, k_2) \\ \Big\downarrow & & \\ \mathrm{Gr}(d, k_2) & & \end{array}$$

Each fiber of the vertical arrow over a point $\xi \in \mathrm{Gr}(d, k_2)$ gives the linear subspace $\mathbb{P}D_\xi \subset \mathbb{P}^{d-1}$ represented by ξ. Via the Segre embedding, we can regard $\phi^{\Gamma(S_2)}(E_1) \times \mathrm{Gr}(d, k_2)$ as a subset of $\mathbb{P}^{d-1} \times \mathrm{Gr}(d, k_2)$. Take the intersection $(\phi^{\Gamma(S_2)}(E_1) \times \mathrm{Gr}(d, k_2)) \cap \mathbb{P}\mathcal{U}_2$. There are obvious projections

$$\begin{array}{ccc} & (\phi^{\Gamma(S_2)}(E_1) \times \mathrm{Gr}(d, k_2)) \cap \mathbb{P}\mathcal{U}_2 & \\ {\scriptstyle p}\swarrow & & \searrow{\scriptstyle q} \\ \phi^{\Gamma(S_2)}(E_1) & & \mathrm{Gr}(d, k_2) \end{array}$$

Let us estimate the dimension of this intersection. For each point η in $\phi^{\Gamma(S_2)}(E_1)$, $p^{-1}(\eta)$ is

$$\{D_2 \in \mathrm{Gr}(d, k_2) \,|\, \eta \in \mathbb{P}D_2\} \cong \mathrm{Gr}(d-1, k_2)$$

since a subspace of $\mathbb{C}^d$ of codimension k_2 containing a line l_η represented by η is uniquely determined by a subspace of $\mathbb{C}^d/l_\eta = \mathbb{C}^{d-1}$ of codimension k_2. Therefore, the intersection $(\phi^{\Gamma(S_2)}(E_1) \times \mathrm{Gr}(d, k_2)) \cap \mathbb{P}\mathcal{U}_2$ is a smooth real manifold of real dimension

$$2(N_U - k_1) + \dim_{\mathbb{R}} \mathrm{Gr}(d-1, k_2) = 2(N_U - k_1) + 2k_2(d-1-k_2).$$

If q is not surjective, the fiber $q^{-1}(D_2) = \phi^{\Gamma(S_2)}(E_1) \cap \iota^{-1}(\mathbb{P}D_2)$ is empty for a generic choice of $D_2 \in \mathrm{Gr}(d, k_2)$. Let $E_2 := \left(\phi^{\Gamma(S_2)}\right)^{-1}\left(\iota^{-1}(\mathbb{P}D_2)\right)$. Then

$$\begin{aligned} E_1 \cap E_2 =& E_1 \cap \left(\phi^{\Gamma(S_2)}\right)^{-1}\left(\iota^{-1}(\mathbb{P}D_2)\right) \\ =& \left(\phi^{\Gamma(S_2)}\right)^{-1}\left(\phi^{\Gamma(S_2)}(E_1) \cap \iota^{-1}(\mathbb{P}D_2)\right) \\ =& \left(\phi^{\Gamma(S_2)}\right)^{-1}\left(q^{-1}(D_2)\right) = \emptyset \end{aligned} \tag{4.9}$$

for such a generic D_2, so we have the statement (i). Thus we may assume that q is surjective.

Applying the Morse-Sard theorem [Hir76, Chapter 3, Theorem 1.3] to the smooth map $q : (\phi^{\Gamma(S_2)}(E_1) \times \mathrm{Gr}(d, k_2)) \cap \mathbb{P}\mathcal{U}_2 \to \mathrm{Gr}(d, k_2)$, we find that over a generic choice of $D_2 \in \mathrm{Gr}(d, k_2)$, the fiber $q^{-1}(D_2)$ of q is a smooth manifold

of real dimension

$$2(N_U - k_1) + 2k_2(d - 1 - k_2) - 2k_2(d - k_2) = 2(N_U - k_1 - k_2).$$

For such a generic D_2, if we let $E_2 := \left(\phi^{\Gamma(S_2)}\right)^{-1}\left(\iota^{-1}(\mathbb{P}D_2)\right)$, then by (4.9), $E_1 \cap E_2 = \left(\phi^{\Gamma(S_2)}\right)^{-1}\left(q^{-1}(D_2)\right)$ is a smooth manifold of expected real dimension $2(N_U - k_1 - k_2)$.

Now it is obvious how to proceed. We consider the universal bundle $\mathcal{U}_3$ over $\mathrm{Gr}(d, k_3)$, the intersection

$$(\phi^{\Gamma(S_3)}(E_1 \cap E_2) \times \mathrm{Gr}(d, k_3)) \cap \mathbb{P}\mathcal{U}_3$$

and the projections to $\phi^{\Gamma(S_3)}(E_1 \cap E_2)$ and $\mathrm{Gr}(d, k_3)$. If the projection to $\mathrm{Gr}(d, k_3)$ is not surjective, then $\phi^{\Gamma(S_3)}(E_1 \cap E_2) \cap \iota^{-1}(\mathbb{P}D_3)$ is empty for a generic $D_3 \in \mathrm{Gr}(d, k_3)$. For such a generic D_3, if we let $E_3 := \left(\phi^{\Gamma(S_3)}\right)^{-1}\left(\iota^{-1}(\mathbb{P}D_3)\right)$,

$$E_1 \cap E_2 \cap E_3 = \left(\phi^{\Gamma(S_3)}\right)^{-1}\left(\phi^{\Gamma(S_3)}(E_1 \cap E_2) \cap \iota^{-1}(\mathbb{P}D_3)\right)$$

is also empty and we have the theorem.

If the projection to $\mathrm{Gr}(d, k_3)$ is surjective, by the Morse-Sard theorem, we find that for a generic $D_3 \in \mathrm{Gr}(d, k_3)$, $\phi^{\Gamma(S_3)}(E_1 \cap E_2) \cap \mathbb{P}D_3$ is a smooth manifold of real dimension $2(N_U - k_1 - k_2 - k_3)$. Then letting $E_3 := \left(\phi^{\Gamma(S_3)}\right)^{-1}\left(\iota^{-1}(\mathbb{P}D_3)\right)$, $E_1 \cap E_2 \cap E_3$ is also a smooth manifold of real dimension $2(N_U - k_1 - k_2 - k_3)$ for such a generic D_3. Continuing this way, the intersection

$$\bigcap_{i=1}^{r} E_i = \bigcap_{i=1}^{r} \left(\phi^{\Gamma(S_i)}\right)^{-1}\left(\iota^{-1}(\mathbb{P}D_i)\right)$$

eventually becomes empty for generic choices of D_i since $N_U < \sum_i k_i = N_E$. This proves (i) of Theorem 4.2.1.

4.3.2 Critical case

For the statements (ii) and (iii), we need the following theorem which gives us an algebraic sufficient condition for the existence of nonzero solutions of the system of equations (4.1).

Theorem 4.3.1. *Let* $\{S_1, \cdots, S_r\}$ *be sequences of subsets of* $[n]$ *and* $\{D_1, \cdots, D_r\}$ *subspaces of* $\mathcal{H} = \bigotimes_{j=1}^{n} \mathbb{C}^{d_j}$ *with* $k_i = \dim\ D_i^{\perp}$. *If*

$$\prod_{i=1}^{r} (\sigma_{i,1}\alpha_1 + \sigma_{i,2}\alpha_2 + \cdots + \sigma_{i,n}\alpha_n)^{k_i} \neq 0 \tag{4.10}$$

in the ring $\mathbb{Z}[\alpha_1, \alpha_2, \cdots, \alpha_n]/(\alpha_1^{d_1}, \alpha_2^{d_2}, \cdots, \alpha_n^{d_n})$, *then the system of equations* (4.1) *has a nonzero solution.*

Proof. Consider the diagram (4.7). We have to measure the size of the set

$$\bigcap_{i=1}^{r} \left(\phi^{\Gamma(S_i)}\right)^{-1} \left(\iota^{-1}(\mathbb{P}D_i)\right) = \left\{ ([|\psi_j\rangle]) \in \prod_{j=1}^{n} \mathbb{P}^{d_j-1} \mid \left(\otimes_{j=1}^{n} |\psi_j\rangle\right)^{\Gamma(S_i)} \in D_i \right\}.$$

The cohomology ring of $\prod_{j=1}^{n} \mathbb{P}^{d_j-1}$ is

$$H^*\left(\prod_{j=1}^{n} \mathbb{P}^{d_j-1}\right) = \mathbb{Z}[\alpha_1, \cdots, \alpha_n]/(\alpha_1^{d_1}, \cdots, \alpha_n^{d_n}).$$

See Section 2.6 for more details. By Bertini's theorem [Har77, Chapter II, Theorem 8.18] again, we can choose perturbations $\mathbb{P}D_i'$ of $\mathbb{P}D_i$ such that $\iota^{-1}(\mathbb{P}D_i')$ are smooth and Poincaré dual to $(\alpha_1 + \cdots + \alpha_n)^{k_i}$ for each $i = 1, 2, \cdots, r$. Since the complex conjugation changes the orientation, the perturbation $\left(\phi^{\Gamma(S_i)}\right)^{-1} \left(\iota^{-1}(\mathbb{P}D_i')\right)$ of $\left(\phi^{\Gamma(S_i)}\right)^{-1} \left(\iota^{-1}(\mathbb{P}D_i)\right)$ is a smooth submanifold of $\prod_{j=1}^{n} \mathbb{P}^{d_j-1}$, whose Poincaré dual is

$$(\sigma_{i,1}\alpha_1 + \sigma_{i,2}\alpha_2 + \cdots + \sigma_{i,n}\alpha_n)^{k_i}.$$

By the transversality theorem [Hir76, Chapter 3, Theorem 2.4] in differential

topology, we can find perturbations W_i in $\prod_{j=1}^{n} \mathbb{P}^{d_j-1}$ of $\left(\phi^{\Gamma(S_i)}\right)^{-1}\left(\iota^{-1}(\mathbb{P}D_i')\right)$ that are still smooth and intersect transversely. Then the Poincaré dual of $\bigcap_{i=1}^{r} W_i$ is the class

$$\prod_{i=1}^{r}(\sigma_{i,1}\alpha_1 + \sigma_{i,2}\alpha_2 + \cdots + \sigma_{i,n}\alpha_n)^{k_i}$$

in the cohomology ring $H^*\left(\prod_{j=1}^{n} \mathbb{P}^{d_j-1}\right) = \mathbb{Z}[\alpha_1, \cdots, \alpha_n]/(\alpha_1^{d_1}, \cdots, \alpha_n^{d_n})$. If the set $\bigcap_{i=1}^{r}\left(\phi^{\Gamma(S_i)}\right)^{-1}\left(\iota^{-1}(\mathbb{P}D_i)\right)$ is empty, so is its small perturbation $\bigcap_{i=1}^{r} W_i$ and hence the cohomology class $\prod_{i=1}^{r}(\sigma_{i,1}\alpha_1 + \sigma_{i,2}\alpha_2 + \cdots + \sigma_{i,n}\alpha_n)^{k_i}$ should be zero. This proves the theorem. □

The statement (ii) of Theorem 4.2.1 is an easy consequence of Theorem 4.3.1. Indeed, $\prod_{i=1}^{r}(\sigma_{i,1}\alpha_1 + \sigma_{i,2}\alpha_2 + \cdots + \sigma_{i,n}\alpha_n)^{k_i}$ in the quotient ring of the polynomial ring $\mathbb{Z}[\alpha_1, \cdots, \alpha_n]$ by the relations $\alpha_1^{d_1} = \cdots = \alpha_n^{d_n} = 0$ should be a constant multiple of $\prod_j \alpha_j^{d_j-1}$, because $N_E = \sum_i k_i = \sum_j (d_j - 1) = N_U$ in the critical case.

It is worthwhile to consider the case when all the subsets $S_i \subset [n]$ are empty. In this case, $\sigma_{i,j} = 1$ for every i, j and

$$\prod_{i=1}^{r}(\sigma_{i,1}\alpha_1 + \sigma_{i,2}\alpha_2 + \cdots + \sigma_{i,n}\alpha_n)^{k_i} = (\alpha_1 + \alpha_2 + \cdots + \alpha_n)^{\Sigma(d_j-1)}.$$

It is straightforward to check that the coefficient of $\prod_j \alpha_j^{d_j-1}$ in the polynomial $(\alpha_1 + \alpha_2 + \cdots + \alpha_n)^{\Sigma(d_j-1)}$ is $\dfrac{\left(\sum_j (d_j - 1)\right)!}{\prod_j (d_j - 1)!} > 0$. We thus obtain the following.

Corollary 4.3.2. *Let $D_1, \cdots, D_r$ be subspaces of $\mathcal{H}$ with $k_i = \dim D_i^{\perp}$ for $i = 1, \cdots, r$. If $\sum_{i=1}^{r} k_i = \sum_j (d_j - 1)$, then we have the following:*

(i) *There always exists a nonzero product vector $|\psi\rangle$ satisfying $|\psi\rangle \in D_i$ for $1 \le i \le r$.*

(ii) *The number of distinct nonzero product vectors* $|\psi\rangle$ *up to constant satisfying* $|\psi\rangle \in D_i$ *for* $1 \leq i \leq r$ *is less than or equal to* $\frac{\left(\sum_j (d_j - 1)\right)!}{\prod_j (d_j - 1)!}$ *if it is finite.*

(iii) *The equality holds for generic choices of* D_i.

We notice that the number $\frac{\left(\sum_j (d_j - 1)\right)!}{\prod_j (d_j - 1)!}$ is nothing but the degree of the Segre variety $Seg(\prod_{j=1}^n \mathbb{P}^{d_j - 1})$. See Section 2.6.

4.3.3 Under-determined case

For the proof of the statement (iii) of Theorem 4.2.1, we introduce some vector notations. For $\mathbf{k} := (k_1, k_2, \cdots, k_r)$, $\mathbf{m} := (m_1, m_2, \cdots, m_n)$ and $\alpha := (\alpha_1, \alpha_2, \cdots, \alpha_n)$, we denote $|\mathbf{k}| := \sum k_i$, $|\mathbf{m}| := \sum m_j$ and $\alpha^{\mathbf{m}} := \prod_{j=1}^n \alpha_j^{m_j}$. Let $\sigma_i := (\sigma_{i,1}, \cdots, \sigma_{i,n}) \in \{-1, +1\}^n$ so that we can write $\sigma_i \cdot \alpha := \sigma_{i,1}\alpha_1 + \sigma_{i,2}\alpha_2 + \cdots + \sigma_{i,n}\alpha_n$. By expanding, we write

$$P^{\mathbf{k}}(\alpha) := \prod_{i=1}^r (\sigma_{i,1}\alpha_1 + \sigma_{i,2}\alpha_2 + \cdots + \sigma_{i,n}\alpha_n)^{k_i} = \sum_{|\mathbf{m}|=|\mathbf{k}|} A_{\mathbf{m}}^{\mathbf{k}} \alpha^{\mathbf{m}}$$

for $A_{\mathbf{m}}^{\mathbf{k}} \in \mathbb{Z}$. For convenience, we define $A_{\mathbf{m}}^{\mathbf{k}}$ to be zero whenever there is a component of $\mathbf{k}$ or $\mathbf{m}$ which is negative. For two vectors $\mathbf{v} = (v_1, v_2, \cdots, v_n)$ and $\mathbf{w} = (w_1, w_2, \cdots, w_n)$ in $\mathbb{Z}^n$, we say $\mathbf{v} \geq \mathbf{w}$ when $v_i \geq w_i$ for all i. We begin with the following:

Proposition 4.3.3. *Let* $D_1, \cdots, D_r$ *be subspaces of* $\mathcal{H} = \bigotimes_{j=1}^n \mathbb{C}^{d_j}$ *with* $k_i = \dim D_i^{\perp}$ *for* $i = 1, \cdots, r$. *If* $N_E = \sum_{i=1}^r k_i < N_U$ *and* $P^{\mathbf{k}}(\alpha) = \prod_{i=1}^r (\sigma_{i,1}\alpha_1 + \sigma_{i,2}\alpha_2 + \cdots + \sigma_{i,n}\alpha_n)^{k_i}$ *is not zero in the ring* $\mathbb{Z}[\alpha]/(\alpha_j^{d_j})_{1 \leq j \leq n}$, *then the system of equations* (4.1) *has infinitely many solutions.*

Proof. Since $P^{\mathbf{k}}(\alpha)$ is the Poincaré dual of a small perturbation of the inter-

section

$$\bigcap_{i=1}^{r} \left(\phi^{\Gamma(S_i)}\right)^{-1} \left(\iota^{-1}(\mathbb{P}D_i)\right) = \left\{ ([|\psi_j\rangle]) \in \prod_{j=1}^{n} \mathbb{P}^{d_j-1} \mid \left(\otimes_{j=1}^{n} |\psi_j\rangle\right)^{\Gamma(S_i)} \in D_i \right\}$$

as shown in the proof of Theorem 4.3.1, the nonvanishing of the class $P^{\mathbf{k}}(\alpha)$ implies that a small perturbation of the intersection is a nonempty smooth manifold of real dimension $2(N_U - \sum_{i=1}^{r} k_i) > 0$. Therefore, the intersection always has infinitely many points and hence we find that there are uncountably many product vectors $|\psi\rangle$ satisfying $|\psi\rangle^{\Gamma(S_i)} \in D_i$. □

The next question is when $P^{\mathbf{k}}(\alpha)$ is nonzero in the ring $\mathbb{Z}[\alpha]/(\alpha_j^{d_j})_{1\le j\le n}$. It was shown in [KKL11, Lemma 2] that $P^{\mathbf{k}}(\alpha)$ is always nonzero in the under-determined case if $n = 2$. However it is not true even for $n = 3$.

Example 4.3.4. Let $n = 3$. Let $S_1 = \{1\}$, $S_2 = \{2\}$, $S_3 = \{3\}$ and $S_4 = \emptyset$. Let $d_1 = d_2 = 2$, $d_3 = 4$, and $k_1 = k_2 = k_3 = k_4 = 1$. Then $N_E = 4 < 5 = N_U$. In the ring $\mathbb{Z}[\alpha]/(\alpha_j^{d_j})$, we have

$$P^{\mathbf{k}}(\alpha) = (-\alpha_1 + \alpha_2 + \alpha_3)(\alpha_1 - \alpha_2 + \alpha_3)(\alpha_1 + \alpha_2 - \alpha_3)(\alpha_1 + \alpha_2 + \alpha_3) = 0$$

since $\alpha_1^2 = \alpha_2^2 = \alpha_3^4 = 0$. Hence $P^{\mathbf{k}}(\alpha)$ may be zero even for the under-determined case when $n = 3$. We note that the associated matrix Σ is given by

$$\begin{pmatrix} - & + & + \\ + & - & + \\ + & + & - \\ + & + & + \end{pmatrix},$$

where $+$ and $-$ denote $+1$ and -1, respectively.

In this example, the matrix Σ has rank smaller than r. This suggests that we may have to impose a condition on the rank of Σ in order to have the nonvanishing of $P^{\mathbf{k}}(\alpha)$. Here is a criterion, and this completes the proof of (iii) of Theorem 4.2.1.

Proposition 4.3.5. *Let* $\Sigma = (\sigma_{i,j})$ *be an* $r \times n$ *matrix whose entries are* ± 1. *Let* $k_1, \cdots, k_r \in \mathbb{Z}_{\geq 0}$ *and* $d_1, \cdots, d_n \in \mathbb{Z}_{>0}$. *If* $\sum_{i=1}^{r} k_i < \sum_{j=1}^{n}(d_j - 1)$ *and the rank of* Σ *is* r, *then* $P^{\mathbf{k}}(\alpha) = \prod_{i=1}^{r}(\sigma_i \cdot \alpha)^{k_i}$ *is nonzero in the ring* $\mathbb{Z}[\alpha]/(\alpha_j^{d_j})_{1 \leq j \leq n}$ *for* $\mathbf{k} \geq 0$.

Proof. We fix $d_1, d_2, \cdots, d_n$, Σ and allow $\mathbf{k}$ to vary. The proposition is equivalent to saying that there is an n-tuple of nonnegative integers $\mathbf{m} := (m_1, m_2, \cdots, m_n)$ such that $|\mathbf{m}| = |\mathbf{k}|$, $m_j \leq d_j - 1$ for every j and $A_{\mathbf{m}}^{\mathbf{k}} \neq 0$ whenever $\sum_{i=1}^{r} k_i < \sum_{j=1}^{n}(d_j - 1)$. This is obvious for $\mathbf{k} = 0$ since $A_{0,0,\cdots,0}^{0,0,\cdots,0} = 1$. Suppose that there is a $\mathbf{k} \geq 0$ for which the proposition fails. Let $\tilde{\mathbf{k}}$ be such a vector with $|\tilde{\mathbf{k}}|$ minimal.

Consider the following statement for nonnegative integers s and m.

$\mathcal{T}_{s,m}^{\mathbf{k}}$: *All the coefficients* $A_{\mathbf{m}}^{\mathbf{k}}$ *are zero whenever* $m_s = m$ *or* $m_s = m + 1$ *and when* $m_j \leq d_j - 1$ *for* $1 \leq j \leq n$.

We claim that *for a fixed* $\mathbf{k}$ *and given* s, *if the statement* $\mathcal{T}_{s,m}^{\mathbf{k}}$ *holds for some* m, *then so does the statement* $\mathcal{T}_{s,m-1}^{\mathbf{k}-\mathbf{e}_i}$ *for every* i, where $\mathbf{e}_i$ denotes the i-th standard basis vector.

This claim induces a contradiction to the minimality of $|\tilde{\mathbf{k}}|$ and hence proves the proposition. Indeed, by the assumption on $\tilde{\mathbf{k}}$, $\mathcal{T}_{s,m}^{\tilde{\mathbf{k}}}$ holds for every s and $m \leq d_s - 2$. Then the claim says that the statement $\mathcal{T}_{s,m}^{\tilde{\mathbf{k}}-\mathbf{e}_i}$ holds for every s and $m \leq d_s - 3$. In particular, $A_{\mathbf{m}}^{\tilde{\mathbf{k}}-\mathbf{e}_i}$ can be nonzero only when $m_s = d_s - 1$ for every s, which is impossible since $|\mathbf{m}| = |\tilde{\mathbf{k}} - \mathbf{e}_i| = |\tilde{\mathbf{k}}| - 1 < \sum(d_j - 1) = N_U$. Therefore, all the $A_{\mathbf{m}}^{\tilde{\mathbf{k}}-\mathbf{e}_i}$ are zero for every $\mathbf{m}$ satisfying $|\mathbf{m}| = |\tilde{\mathbf{k}}| - 1$ and $m_j \leq d_j - 1$. This contradicts the minimality of $|\tilde{\mathbf{k}}|$.

Now we prove the claim. Suppose that the statement $\mathcal{T}_{s,m}^{\mathbf{k}}$ holds for some s and m. For each j, we take the partial derivative of $P^{\mathbf{k}} := P^{\mathbf{k}}(\alpha)$ with respect to α_j to obtain the following:

$$\frac{\partial}{\partial \alpha_j} P^{\mathbf{k}} = \sum_{i=1}^{r} k_i \sigma_{i,j} P^{\mathbf{k}-\mathbf{e}_i} = \sum_{i=1}^{r} k_i \sigma_{i,j} \left(\sum_{|\mathbf{m}'|=|\mathbf{k}-\mathbf{e}_i|} A_{\mathbf{m}'}^{\mathbf{k}-\mathbf{e}_i} \alpha^{\mathbf{m}'} \right) = \sum_{|\mathbf{m}|=|\mathbf{k}|} m_j A_{\mathbf{m}}^{\mathbf{k}} \alpha^{\mathbf{m}-\mathbf{e}_j}.$$

We fix an integer ℓ. If we take the coefficient of the monomial $\alpha^{\mathbf{m}-\mathbf{e}_\ell}$ of the equation above for each j, we get the following system of equations:

$$\begin{array}{rcccccc}
m_1 A^{\mathbf{k}}_{\mathbf{m}+\mathbf{e}_1-\mathbf{e}_\ell} &=& k_1\sigma_{1,1}A^{\mathbf{k}-\mathbf{e}_1}_{\mathbf{m}-\mathbf{e}_\ell} &+& k_2\sigma_{2,1}A^{\mathbf{k}-\mathbf{e}_2}_{\mathbf{m}-\mathbf{e}_\ell} &+\cdots+& k_r\sigma_{r,1}A^{\mathbf{k}-\mathbf{e}_r}_{\mathbf{m}-\mathbf{e}_\ell}\\
m_2 A^{\mathbf{k}}_{\mathbf{m}+\mathbf{e}_2-\mathbf{e}_\ell} &=& k_1\sigma_{1,2}A^{\mathbf{k}-\mathbf{e}_1}_{\mathbf{m}-\mathbf{e}_\ell} &+& k_2\sigma_{2,2}A^{\mathbf{k}-\mathbf{e}_2}_{\mathbf{m}-\mathbf{e}_\ell} &+\cdots+& k_r\sigma_{r,2}A^{\mathbf{k}-\mathbf{e}_r}_{\mathbf{m}-\mathbf{e}_\ell}\\
&& \cdots &&&&\\
m_{\ell-1} A^{\mathbf{k}}_{\mathbf{m}+\mathbf{e}_{\ell-1}-\mathbf{e}_\ell} &=& k_1\sigma_{1,\ell-1}A^{\mathbf{k}-\mathbf{e}_1}_{\mathbf{m}-\mathbf{e}_\ell} &+& k_2\sigma_{2,\ell-1}A^{\mathbf{k}-\mathbf{e}_2}_{\mathbf{m}-\mathbf{e}_\ell} &+\cdots+& k_r\sigma_{r,\ell-1}A^{\mathbf{k}-\mathbf{e}_r}_{\mathbf{m}-\mathbf{e}_\ell}\\
m_\ell A^{\mathbf{k}}_{\mathbf{m}} &=& k_1\sigma_{1,\ell}A^{\mathbf{k}-\mathbf{e}_1}_{\mathbf{m}-\mathbf{e}_\ell} &+& k_2\sigma_{2,\ell}A^{\mathbf{k}-\mathbf{e}_2}_{\mathbf{m}-\mathbf{e}_\ell} &+\cdots+& k_r\sigma_{r,\ell}A^{\mathbf{k}-\mathbf{e}_r}_{\mathbf{m}-\mathbf{e}_\ell}\\
m_{\ell+1} A^{\mathbf{k}}_{\mathbf{m}+\mathbf{e}_{\ell+1}-\mathbf{e}_\ell} &=& k_1\sigma_{1,\ell+1}A^{\mathbf{k}-\mathbf{e}_1}_{\mathbf{m}-\mathbf{e}_\ell} &+& k_2\sigma_{2,\ell+1}A^{\mathbf{k}-\mathbf{e}_2}_{\mathbf{m}-\mathbf{e}_\ell} &+\cdots+& k_r\sigma_{r,\ell+1}A^{\mathbf{k}-\mathbf{e}_r}_{\mathbf{m}-\mathbf{e}_\ell}\\
&& \cdots &&&&\\
m_n A^{\mathbf{k}}_{\mathbf{m}+\mathbf{e}_n-\mathbf{e}_\ell} &=& k_1\sigma_{1,n}A^{\mathbf{k}-\mathbf{e}_1}_{\mathbf{m}-\mathbf{e}_\ell} &+& k_2\sigma_{2,n}A^{\mathbf{k}-\mathbf{e}_2}_{\mathbf{m}-\mathbf{e}_\ell} &+\cdots+& k_r\sigma_{r,n}A^{\mathbf{k}-\mathbf{e}_r}_{\mathbf{m}-\mathbf{e}_\ell}
\end{array}$$

If $m_s = m$ and $\ell \neq s$, or $m_s = m+1$ and $\ell = s$, then LHS are all zero by assumption. Therefore, we have

$$\begin{pmatrix} & \vdots & \\ — & k_1\sigma_{1,j} & — \\ — & k_2\sigma_{2,j} & — \\ & \cdots & \\ — & k_r\sigma_{r,j} & — \\ & \vdots & \end{pmatrix}^t \cdot \begin{pmatrix} \vdots \\ A^{\mathbf{k}-\mathbf{e}_1}_{\mathbf{m}-\mathbf{e}_\ell} \\ A^{\mathbf{k}-\mathbf{e}_2}_{\mathbf{m}-\mathbf{e}_\ell} \\ \vdots \\ A^{\mathbf{k}-\mathbf{e}_r}_{\mathbf{m}-\mathbf{e}_\ell} \\ \vdots \end{pmatrix} = O.$$

Since the matrix $(\sigma_{i,j})$ has rank r, so does the matrix $(k_i\sigma_{i,j})^t$ whenever all the $k_i \neq 0$. Hence, all the $A^{\mathbf{k}-\mathbf{e}_i}_{\mathbf{m}'}$ are zero for any i when the s-th component m'_s of $\mathbf{m}'$ is m and $k_i \neq 0$ for all i. If some k_i is zero, we can simply remove the i-th column from the matrix $(k_i\sigma_{i,j})^t$ and $A^{\mathbf{k}-\mathbf{e}_i}_{\mathbf{m}-\mathbf{e}_\ell}$ from the column vector because $A^{\mathbf{k}-\mathbf{e}_i}_{\mathbf{m}-\mathbf{e}_\ell} = 0$ by our convention. The modified matrix of $(k_i\sigma_{i,j})^t$ has full rank as well, so the column vector must be also zero. Therefore, all the $A^{\mathbf{k}-\mathbf{e}_i}_{\mathbf{m}'}$ are zero for every i and $\mathbf{m}'$ with $m'_s = m$ and $|\mathbf{m}'| = |\mathbf{k}| - 1$.

Now, we claim that $A^{\mathbf{k}-\mathbf{e}_i}_{\mathbf{m}'}$ are zero for any i when $m'_s = m-1$. By expanding $P^{\mathbf{k}}(\alpha)$ directly, we obtain the following:

$$A^{\mathbf{k}}_{\mathbf{m}} = \sum_{m_j = \sum_i k_{i,j}} \prod_{i=1}^{r} \binom{k_i}{\mathbf{k}_i} \prod_{j=1}^{n} \sigma_{i,j}^{k_{i,j}},$$

where $\mathbf{k}_i := (k_{i,1}, k_{i,2}, \cdots, k_{i,n})$ and $\binom{k_i}{\mathbf{k}_i} := \frac{k_i!}{\prod_j (k_{i,j}!)}$ when $k_{i,j} \geq 0$ and $k_i = |\mathbf{k}_i|$. We let $\binom{k_i}{\mathbf{k}_i} = 0$ if some $k_{i,j} < 0$. Since $\binom{k_i}{\mathbf{k}_i} = \sum_j \binom{k_i - 1}{\mathbf{k}_i - \mathbf{e}_j}$,

$$A^{\mathbf{k}}_{\mathbf{m}} = \sigma_{1,j} A^{\mathbf{k}-\mathbf{e}_j}_{\mathbf{m}-\mathbf{e}_1} + \sigma_{2,j} A^{\mathbf{k}-\mathbf{e}_j}_{\mathbf{m}-\mathbf{e}_2} + \cdots + \sigma_{n,j} A^{\mathbf{k}-\mathbf{e}_j}_{\mathbf{m}-\mathbf{e}_n} \quad \text{for each } j.$$

Note that if $m_s = m$, then $A^{\mathbf{k}}_{\mathbf{m}}$ and $A^{\mathbf{k}-\mathbf{e}_j}_{\mathbf{m}-\mathbf{e}_i}$ are zero for $i \neq s$. We thus have $A^{\mathbf{k}-\mathbf{e}_j}_{\mathbf{m}-\mathbf{e}_s} = 0$ for every j and $\mathbf{m}$ with $m_s = m$. Therefore, all the $A^{\mathbf{k}-\mathbf{e}_i}_{\mathbf{m}'}$ are zero for any i when the s-th component of $\mathbf{m}'$ is $m-1$ or m. We thus proved the statement $\mathcal{T}^{\mathbf{k}-\mathbf{e}_i}_{s,m-1}$ for every i. This completes the proof. □

In order to apply Theorem 4.2.1 (iii), it helps to minimize the number r in the system of equations (4.1). To do this, we may assume that the associated matrix Σ has pairwisely non-parallel rows. Indeed, if $S_i = S_j$ (respectively $S_i = S_j^c$) for some $i \neq j$, then we can combine two systems of equations $|\psi\rangle^{\Gamma(S_i)} \in D_i$ and $|\psi\rangle^{\Gamma(S_j)} \in D_j$ into a single $|\psi\rangle^{\Gamma(S_i)} \in D_i \cap D_j$ (respectively $|\psi\rangle^{\Gamma(S_i)} \in D_i \cap \bar{D}_j$). If $r \leq 3$, then it is easy to see that pairwisely non-parallel rows of Σ are always linearly independent. Therefore, the rank condition in Proposition 4.3.5 is automatically satisfied. This is not true for $r = 4$, as we have seen in Example 4.3.4.

If $n = 2$, then we may always assume that $r \leq 2$ by the above argument, so the rank condition is redundant. For the n qubit under-determined cases, we have $r \leq N_E < N_U = n$, so the rank condition is also redundant for the three or four qubit cases because $r \leq 3$. Therefore, we have the following. The case of $n = 2$ is nothing but [KKL11, Theorem 3, (ii)].

Proposition 4.3.6. *Let $n = 2$ or $d_j = 2$ with $n = 3, 4$. Then the system of equations (4.1) has infinitely many solutions whenever $N_E < N_U$.*

It is worthwhile to note that the converse of Proposition 4.3.5 does not hold. To see this, we consider the following two matrices in the five qubit

case with $k_j = 1$ for $j = 1, 2, 3, 4$:

$$\Sigma_1 = \begin{pmatrix} - & + & + & - & - \\ + & - & + & + & + \\ + & + & - & + & + \\ + & + & + & + & + \end{pmatrix}, \qquad \Sigma_2 = \begin{pmatrix} - & + & + & - & + \\ + & - & + & + & - \\ + & + & - & + & + \\ + & + & + & + & + \end{pmatrix}.$$

These are of rank three. It is interesting to note that $P^{\mathbf{k}}(\alpha) = 0$ for Σ_1, but $P^{\mathbf{k}}(\alpha)$ is nonzero for Σ_2 in the ring $\mathbb{Z}[\alpha_1, \cdots, \alpha_5]/(\alpha_1^2, \cdots, \alpha_5^2)$. Therefore, the converse of Proposition 4.3.5 does not hold.

In the trivial case where $S_i \subset [n]$ are all empty or $[n]$, $P^{\mathbf{k}}(\alpha) = \pm(\alpha_1 + \cdots + \alpha_n)^{N_E}$ is always nonzero because $N_E < N_U$ and $(\alpha_1 + \cdots + \alpha_n)^{N_U} \neq 0$ in $\mathbb{Z}[\alpha]/(\alpha_j^{d_j})$ by Corollary 4.3.2. By Proposition 4.3.3, the system of equations (4.1) has infinitely many nonzero solutions for any D_i with $\dim D_i^{\perp} = k_i$.

4.4 Multi-qubit cases and permanents of matrices

In this section, we investigate the multi-qubit cases where $d_j = 2$ for all j so that $N_U = n$. In the critical case where the numbers of equations N_E and unknowns N_U coincide in the system of equations (4.1), we may assume that $k_i = 1$ for all i because if $k_i > 1$ we can repeat S_i k_i times and replace D_i by k_i hyperplanes. In particular, we may assume $N_E = r = n = N_U$. By Theorem 4.2.1 (ii), the solvability of (4.1) is guaranteed by the nonvanishing of the coefficient of the monomial $\alpha_1\alpha_2\cdots\alpha_n$ in the polynomial (4.6), which is

$$\sum_{\lambda \in S_n} \sigma_{1,\lambda(1)}\sigma_{2,\lambda(2)}\cdots\sigma_{n,\lambda(n)}, \tag{4.11}$$

where S_n denotes the set of all permutations of the set $[n]$. If we multiply the sign of permutation in each summand, this is nothing but the determinant of the matrix $\Sigma = [\sigma_{i,j}]$. The number (4.11) is called the permanent, denoted by $\mathrm{per}(\Sigma)$, of the matrix Σ. See Section 2.11. By Theorem 4.2.1 (ii), we have

the following:

Theorem 4.4.1. *Let* $\{S_1, \cdots, S_n\}$ *be subsets of* $[n]$ *with the associated* $n \times n$ *matrix* Σ*, and* $\{D_1, \cdots, D_n\}$ *subspaces of* $\bigotimes_{i=1}^{n} \mathbb{C}^2$ *with* $\dim D_i^{\perp} = 1$ *for* $i = 1, \cdots, n$*, respectively. If* $\mathrm{per}(\Sigma) \neq 0$ *then the system of equations* (4.1) *has a nonzero solution.*

Therefore, in order to check the existence of a nonzero solution of (4.1) for the n qubit cases with the same numbers of equations and unknowns, we have to calculate the permanents of the associated matrices whose entries are ± 1. Several authors have studied permanents of those matrices. It was shown in [Wan74] that if $n \geq 2$ is even or $n \equiv 1 (\mathrm{mod}\ 4)$, then there exists an $n \times n$ $(+1, -1)$-matrix A with $\mathrm{per}(A) = 0$. In the same paper, it was also noticed that there is no 3×3 $(+1, -1)$-matrix with vanishing permanent. It was proved in [KS83, SS83, Wan05] that there exists an $n \times n$ $(+1, -1)$-matrix with vanishing permanent if and only if $n + 1$ is not a power of 2. Therefore, we have the following:

Theorem 4.4.2. *Let* $n = 2^k - 1$ *for* $k = 2, 3, \cdots$ *and* $d_i = 2$ *for* $i = 1, 2, \cdots, n$*. Then the system of equations* (4.1) *has a nonzero solution whenever the number of equations are less than or equal to* n*.*

The above theorem does not hold even for the two qubit case with $n = 2$. See Example 4.1.3. Since $S_1 = \{2\}$, $S_2 = \emptyset$ in the condition (4.4), the associated matrix is given by

$$\begin{pmatrix} + & - \\ + & + \end{pmatrix}.$$

We note that the permanent of the associated matrix vanishes. We modify this example to get the same kind of a system of equations for the four qubit case with the same number of equations and unknowns.

Example 4.4.3. Let subspaces $\{D_1, D_2, D_3, D_4\}$ of $\bigotimes_{j=1}^{4} \mathbb{C}^2$ be given by

$$D_1 = (|\beta_1\rangle \otimes |\beta_1\rangle)^{\perp},\ D_2 = (|\beta_1\rangle \otimes |\beta_2\rangle)^{\perp},\ D_3 = (|\beta_2\rangle \otimes |\beta_1\rangle)^{\perp},\ D_4 = (|\beta_2\rangle \otimes |\beta_2\rangle)^{\perp}.$$

Then, we have

$$\begin{array}{lcll} |\psi_1,\bar{\psi}_2\rangle\otimes|\psi_3,\bar{\psi}_4\rangle\in D_1 & \Longleftrightarrow & |\psi_1\rangle\perp|\psi_2\rangle \quad \text{or} & |\psi_3\rangle\perp|\psi_4\rangle \\ |\psi_1,\bar{\psi}_2\rangle\otimes|\psi_3,\psi_4\rangle\in D_2 & \Longleftrightarrow & |\psi_1\rangle\perp|\psi_2\rangle \quad \text{or} & |\psi_3\rangle\parallel|\psi_4\rangle \\ |\psi_1,\psi_2\rangle\otimes|\psi_3,\bar{\psi}_4\rangle\in D_3 & \Longleftrightarrow & |\psi_1\rangle\parallel|\psi_2\rangle \quad \text{or} & |\psi_3\rangle\perp|\psi_4\rangle \\ |\psi_1,\psi_2\rangle\otimes|\psi_3,\psi_4\rangle\in D_4 & \Longleftrightarrow & |\psi_1\rangle\parallel|\psi_2\rangle \quad \text{or} & |\psi_3\rangle\parallel|\psi_4\rangle \end{array} \tag{4.12}$$

It is clear that there exists no nonzero product vector $|\psi_1,\psi_2,\psi_3,\psi_4\rangle\in\bigotimes_{j=1}^{4}\mathbb{C}^2$ satisfying all of these equations. Note the the associated matrix is

$$\begin{pmatrix} + & - & + & - \\ + & - & + & + \\ + & + & + & - \\ + & + & + & + \end{pmatrix},$$

which has the vanishing permanent. If we take the last three columns then it is equivalent to the associated matrix in Example 4.3.4. Employing the above method to construct the example for $n=4$ from the example for $n=2$, it is easy to construct the same kind of examples when $n=2^k$ for $k\geq 3$.

We say that two $r\times n$ matrices Σ_1 and Σ_2 are equivalent if Σ_2 is obtained from Σ_1 by a succession of the following operations:

(i) interchange two rows or columns,

(ii) negate a row or a column.

Interchanging two rows and columns is equivalent to changing the orders of equations and unknowns in (4.1), and negating a row or a column is equivalent to conjugating an equation or an unknown in (4.1). Therefore, two systems of equations like (4.1) have the same solvability if their associated matrices are equivalent.

It is a natural problem to classify all $n\times n$ $(+1,-1)$-matrices with vanishing permanents, up to equivalence. The first step for classification is to

reduce the number $\mu(\Sigma)$ of minus signs, that is, the number of -1's in the entries of Σ. We also denote by $r_i(\Sigma)$ (respectively $c_j(\Sigma)$) the number of minus signs in the i-th row (respectively the j-th column) of Σ.

Proposition 4.4.4. *Suppose that $n \geq 3$. For a given $n \times n$ matrix $\Sigma = [\sigma_{ij}]$ with entries ± 1, we have the following:*

(i) *If $n = 2m+1$ is an odd number and $\mu(\Sigma) \geq mn-(m-1)$, then there exists Σ' which is equivalent to Σ such that $\mu(\Sigma') < \mu(\Sigma)$.*

(ii) *If $n = 2m$ is an even number and $\mu(\Sigma) \geq mn - m$, then there exists Σ' which is equivalent to Σ such that $\mu(\Sigma') < \mu(\Sigma)$.*

Proof. If there is a column with $m+1$ minus signs then we may decrease the number $\mu(\Sigma)$ strictly by negating this column, and the same for rows. Therefore, it remains to consider the case when all the columns and rows have at most m minus signs. Put

$$I = \{i \in [n] : r_i(\Sigma) = m\}, \qquad J = \{j :\in [n] : c_j(\Sigma) = m\}.$$

We note that if $|I| \leq \ell$ then

$$\mu(\Sigma) \leq m \cdot |I| + (m-1)(n-|I|) = mn - n + |I| \leq mn - n + \ell,$$

and the same for J, where $|I|$ denotes the cardinality of I. Therefore, we have

$$\mu(\Sigma) \geq mn - n + \ell \implies |I| \geq \ell,\ |J| \geq \ell.$$

In case of (i), we have $mn-(m-1) = mn-n+(m+2)$, and so it follows that $|J| \geq m+2$ by assumption. Therefore, for any $i \in I$, there exist at least two $j \in J$, say $\{j_1, j_2\}$, with $\sigma_{ij} = +1$. Take any $i \in I$ and negate the i-th row, to get Σ' with $\mu(\Sigma') = \mu(\Sigma)+1$. If we negate the j_1-th and j_2-th columns to get Σ'', then we have $\mu(\Sigma'') \leq \mu(\Sigma') - 2 = \mu(\Sigma) - 1$.

In the even case $n = 2m$, we first consider the case $\mu(\Sigma) \geq mn-(m-1) = mn-n+(m+1)$. In this case, we have $|J| \geq m+1$, and so for any $i \in I$ there exists at least one $j \in J$ with $\sigma_{ij} = +1$. We apply the same

argument as in the odd n case, to get Σ' and Σ''. In this case, we have $\mu(\Sigma'') \leq \mu(\Sigma') - 1 = \mu(\Sigma) - 1$.

It remains to prove when $n = 2m$ and $\mu(\Sigma) = mn - m$, which implies $|I| \geq m$ and $|J| \geq m$. In this case, we consider the set $I \times J$. If there exists $(i, j) \in I \times J$ with $\sigma_{ij} = +1$ then negate the i-row and the j-th column, to get the conclusion. If $\sigma_{ij} = -1$ for each $(i, j) \in I \times J$ then we see that $|I| = |J| = m$. In this case we negate the i-th row for each $i \in I$ to get Σ'. Then there exist $j \in [n] \setminus J$ such that $c_j(\Sigma') > m$ since $\mu(\Sigma) > |I \times J|$ by the assumption $n \geq 3$. Negate this column to get the required conclusion. □

When n is a power of 2, the following proposition is also useful for classification of $(+1, -1)$-matrices with vanishing permanents. We recall the following addition formula for permanents (Theorem 2.11.2):

$$\operatorname{per}(A + B) = \sum_{i=0}^{n} \sum_{\substack{S,T \in [n] \\ |S|=|T|=i}} \operatorname{per}(A[S|T]) \operatorname{per}(B(S|T)),$$

where $A[S|T]$ is the submatrix of A consisting of rows indexed by S and columns indexed by T, and $B(S|T)$ is the submatrix of B deleting rows indexed by S and columns indexed by T. If $|S| = |T| = 0$ (respectively $|S| = |T| = n$), we set $\operatorname{per}(A[S|T]) = 1$ (respectively $\operatorname{per}(B(S|T)) = 1$). This formula holds for arbitrary $n \times n$ matrices A and B.

Proposition 4.4.5. *Suppose that $n = 2^k$ for $k = 2, 3, \cdots$. If an $n \times n$ matrix Σ with entries ± 1 has the vanishing permanent, then $\mu(\Sigma)$ must be even.*

Proof. We write the $n \times n$ matrix $\Sigma = [\sigma_{i,j}]$ as $J - 2P$ where J is the matrix whose entries are all $+1$ and P is a uniquely determined matrix whose entries are 0 or $+1$. By the addition formula, we obtain the formula

$$\operatorname{per}(\Sigma) = \sum_{i=0}^{n} (-2)^i (n - i)! \operatorname{per}_i(P),$$

where $\operatorname{per}_i(P)$ is the sum of all permanents of $i \times i$ submatrices of P. See

[SS83]. The largest natural number N_i such that 2^{N_i} divides the i-th summand $(-2)^i(n-i)!$ is given by

$$N_i = \begin{cases} n-1, & i = 0, \\ n-k, & i = 1, \\ i + \sum_{j=1}^{k} \left\lfloor \frac{n-i}{2^j} \right\rfloor & i = 2, 3, \cdots, n, \end{cases}$$

where $\lfloor x \rfloor$ is the largest integer which is not greater than x. We show that $N_i \geq n-k+1$ for $i = 2, 3, \cdots, n$. Let $n-i = a_{k-1}2^{k-1} + a_{k-2}2^{k-2} + \cdots + a_0$ be the 2-adic expansion of $n-i$. Then we have $\sum_{j=0}^{k-1} a_j \leq k-1$, because some of a_i must be zero by $i \geq 2$. It is easy to see

$$\sum_{j=1}^{k} \left\lfloor \frac{n-i}{2^j} \right\rfloor = n - i - \sum_{j=0}^{k-1} a_j.$$

Therefore, we have $N_i = n - \sum_{j=0}^{k-1} a_j \geq n-k+1$, and so

$$\mathrm{per}\Sigma \equiv (-2)(n-1)! \cdot \mathrm{per}_1(P) \equiv 2^{n-k}\ell \cdot \mathrm{per}_1(P) \mod 2^{n-k+1},$$

where ℓ is an odd number. Since $\mathrm{per}\Sigma = 0$, we see that $\mu(\Sigma) = \mathrm{per}_1(P)$ must be an even number. □

In order to classify 4×4 $(+1,-1)$-matrices with vanishing permanents up to equivalence, we may consider only the cases $\mu = 2$ and $\mu = 4$, by Propositions 4.4.4 and 4.4.5. In the case of $\mu = 2$, one can check that we have only two permanent vanishing matrices up to equivalence:

$$\Sigma_1 = \begin{pmatrix} - & - & + & + \\ + & + & + & + \\ + & + & + & + \\ + & + & + & + \end{pmatrix},$$

and its transpose Σ_1^t.

In the case of $\mu = 4$, we have to investigate the following cases:

(i) there are two rows with two -1's,

(ii) there are one row with two -1's and two rows with one -1,

(iii) there are four rows with one -1.

In the case of (i), there is only one matrix with vanishing permanent up to equivalence:

$$\Sigma_2 = \begin{pmatrix} - & - & + & + \\ + & - & - & + \\ + & + & + & + \\ + & + & + & + \end{pmatrix}.$$

In the case of (ii), there are only three matrices with vanishing permanents up to equivalence:

$$\Sigma_2^t = \begin{pmatrix} - & + & + & + \\ - & - & + & + \\ + & - & + & + \\ + & + & + & + \end{pmatrix}, \qquad \Sigma_3 = \begin{pmatrix} - & - & + & + \\ + & - & + & + \\ + & + & - & + \\ + & + & + & + \end{pmatrix}, \qquad \Sigma_4 = \begin{pmatrix} - & - & + & + \\ + & + & - & + \\ + & + & + & - \\ + & + & + & + \end{pmatrix}.$$

We note that Σ_2^t is equivalent to the associated matrix in Example 4.4.3 and the transpose of Σ_3 is equivalent to Σ_3 itself. In the case of (iii), there is only one matrix Σ_4^t with vanishing permanent. If we negate the first row of Σ_4 and rearrange the rows and columns appropriately, then we get the matrix Σ_2^t. Therefore, Σ_4 is equivalent to Σ_2^t. This implies that Σ_4^t is also equivalent to Σ_2. To summarize, we have at most five inequivalent $(+1,-1)$-matrices with vanishing permanents up to equivalence:

$$\Sigma_1, \quad \Sigma_1^t, \quad \Sigma_2, \quad \Sigma_2^t, \quad \Sigma_3.$$

We claim that these five matrices are inequivalent. Since Σ_i and Σ_i^t have rank $i+1$ for $i = 1, 2, 3$, we find that neither Σ_i nor Σ_i^t is equivalent to Σ_j or Σ_j^t if $i \neq j$. It remains to show that Σ_1 (respectively Σ_2) and Σ_1^t (respectively Σ_2^t) are not equivalent.

In other to get another invariant to distinguish them, we consider the difference $\pi_r(\Sigma)$ of the two numbers $|\{i \in [n] : r_i(\Sigma) \text{ is even}\}|$ and $|\{i \in [n] : r_i(\Sigma) \text{ is odd}\}|$ for an $n \times n$ matrix Σ with entries ± 1. If n is even then it is easily checked that the number $\pi_r(\Sigma)$ is an invariant under the equivalence relation. The number $\pi_c(\Sigma)$ may be defined for columns in the same way. Since $\pi_r(\Sigma_1) = 4$ and $\pi_r(\Sigma_1^t) = 0$, Σ_1 and Σ_1^t are not equivalent. Similarly, we also check $\pi_r(\Sigma_2) = 4$ and $\pi_r(\Sigma_2^t) = 0$, to confirm that Σ_2 is not equivalent to Σ_2^t.

Theorem 4.4.6. *There exist exactly five* 4×4 $(+1, -1)$*-matrices*

$$\Sigma_1, \quad \Sigma_1^t, \quad \Sigma_2, \quad \Sigma_2^t, \quad \Sigma_3$$

with vanishing permanents, up to the equivalence relation.

We have considered the rank and the invariant $\pi_r(\Sigma)$ to classify permanent vanishing $(+1, -1)$-matrices in the 4×4 cases. The absolute values of the determinant and permanent are also obvious invariants under the equivalence relation. The following example shows that these do not constitute a complete set of invariants.

Example 4.4.7. Consider the following two matrices:

$$A = \begin{pmatrix} - & - & + & + \\ + & - & - & + \\ - & + & - & + \\ + & + & + & + \end{pmatrix}, \qquad B = \begin{pmatrix} + & + & + & + \\ + & - & + & - \\ + & + & - & - \\ + & - & - & + \end{pmatrix}.$$

We can check that

$$\begin{aligned} &\operatorname{per}(A) = \operatorname{per}(B) = 8, \\ &|\det(A)| = |\det(B)| = 16, \\ &\operatorname{rank}(A) = \operatorname{rank}(B) = 4, \\ &\pi_r(A) = \pi_r(B) = \pi_c(A) = \pi_c(B) = 4. \end{aligned}$$

Note that $BB^t = 4I_4$, where I_4 is the 4×4 identity matrix. It is easy to see that if B' is equivalent to B, then $B'B'^t$ is also 4 times the identity matrix. Since $AA^t \neq 4I_4$, A is not equivalent to B.

We close this section by mentioning an interesting asymptotic result on permanents by Tao and Vu [TV09]. For the $n \times n$ matrix M_n whose entries are independent and identically distributed random variables taking values ± 1 with probability $1/2$ for each, they showed that asymptotically almost surely, the absolute value of $\mathrm{per}(M_n)$ is $n^{(\frac{1}{2}+o(1))n}$. In particular, the probability that $\mathrm{per}(M_n) = 0$ tends to 0, as $n \to \infty$.

Chapter 5

Upper Bounds for the Number of Product Vectors

By the range criterion, if a PPT state ρ on $\mathbb{C}^m \otimes \mathbb{C}^n$ is separable, then there is a collection of nonzero product vectors $\left\{|\psi_1^{(i)}\rangle \otimes |\psi_2^{(i)}\rangle\right\}_{i\in I}$ in $\mathbb{C}^m \otimes \mathbb{C}^n$ such that

(i) the range $\mathcal{R}(\rho)$ is spanned by $\left\{|\psi_1^{(i)}\rangle \otimes |\psi_2^{(i)}\rangle\right\}_{i\in I}$,

(ii) the range $\mathcal{R}(\rho^\Gamma)$ is spanned by $\left\{|\overline{\psi_1}^{(i)}\rangle \otimes |\psi_2^{(i)}\rangle\right\}_{i\in I}$.

This leads us to study the following questions: Is there a nonzero product vector $|\psi_1\rangle \otimes |\psi_2\rangle \in \mathbb{C}^m \otimes \mathbb{C}^n$ satisfying the condition

$$|\psi_1\rangle \otimes |\psi_2\rangle \in D, \qquad |\overline{\psi_1}\rangle \otimes |\psi_2\rangle \in E \tag{5.1}$$

for given subspaces D and E of $\mathbb{C}^m \otimes \mathbb{C}^n$? If it exists, how many different product vectors are there satisfying the condition?

In Chapter 4, we proposed a sufficient condition for which there is a nonzero product vector satisfying 5.1. It gives rise to the algebraic criterion for separability which gives us a sufficient condition for a given PPT state to be entangled or almost surely entangled.

In this chapter, we further investigate how many nonzero product vectors with (5.1) exist up to constant. In the previous chapter, we mainly use the homological method of intersection theory in Section 2.3 to investigate the condition (5.1). However, the homological method used to prove the algebraic criterion has some disadvantages. If all the cycles intersect positively, the length of a zero cycle is exactly the same as the intersection number. But if not, the length of a zero cycle would be strictly less than the intersection number. Moreover, it may be zero even if the actual intersection number is not.

So, we try to manipulate the equations directly arising from the range criterion instead of using the homological method in this chapter. These attempts allow us to improve the results 4.1.1 for the qubit-qunit cases and estimate how many different product vectors up to constant exist in $\mathcal{R}(\rho)$ with their partial conjugates in $\mathcal{R}(\rho^\Gamma)$. We will always count distinct nonzero product vectors up to constant unless otherwise specified.

5.1 Transformed into a system of equations

Let $\dim D^\perp = k$ and $\dim E^\perp = \ell$. Then we can write D and E explicitly as follows.

$$D = \left\{ (z_{ij}) \;\middle|\; \sum_{i,j} A_{ij}^{(s)} z_{ij} = 0 \text{ for } 1 \le s \le k,\ A_{ij}^{(s)} \in \mathbb{C} \right\},$$
$$E = \left\{ (z_{ij}) \;\middle|\; \sum_{i,j} B_{ij}^{(t)} z_{ij} = 0 \text{ for } 1 \le t \le \ell,\ B_{ij}^{(t)} \in \mathbb{C} \right\},$$

where (z_{ij}) is the coordinate of the set $M_{m\times n}(\mathbb{C}) \cong \mathbb{C}^m \otimes \mathbb{C}^n$ of all $m \times n$ complex matrices. Then the condition (5.1) is equivalent to the following system of equations:

$$\begin{array}{lll} |\psi_1\rangle \otimes |\psi_2\rangle \in D & \Leftrightarrow & \sum_{i,j} A_{ij}^{(s)} x_i y_j = 0 \text{ for every } 1 \le s \le k, \\ |\overline{\psi_1}\rangle \otimes |\psi_2\rangle \in E & \Leftrightarrow & \sum_{i,j} B_{ij}^{(t)} \bar{x}_i y_j = 0 \text{ for every } 1 \le s \le \ell, \end{array} \tag{5.2}$$

where $|\psi_1\rangle = (x_i) \in \mathbb{C}^m$ and $|\psi_2\rangle = (y_j) \in \mathbb{C}^n$. Since we identify the vectors in $\mathbb{C}^m$ or $\mathbb{C}^n$ up to constant, we can consider $|\psi_1\rangle$ and $|\psi_2\rangle$ as elements in $\mathbb{P}^{m-1}$ and $\mathbb{P}^{n-1}$ respectively. In the system of equations (5.2), we note that the number of equations and that of variables are $k+\ell$ and $m+n-2$ respectively. Hence, it is natural to divide the problem into the following three cases:

- Over-determined case: $k+\ell > m+n-2$
- Critical case : $k+\ell = m+n-2$
- Under-determined case : $k+\ell < m+n-2$

Throughout this chapter, we concentrate only on the critical case, i.e. $k+\ell = m+n-2$ because for the other cases, the number of nonzero product vectors satisfying the condition (5.1) is almost surely zero or infinite by Theorem 4.1.1. In particular, the over-determined case can be studied by the critical case if we replace the given subspace D with a subspace of codimension $m+n-l-2$ containing D. For the critical case, all the equations (5.1) are listed as follows:

$$\begin{aligned} y_1 L_1^{(1)} + y_2 L_2^{(1)} + \cdots + y_n L_n^{(1)} &= 0 \\ y_1 L_1^{(2)} + y_2 L_2^{(2)} + \cdots + y_n L_n^{(2)} &= 0 \\ &\vdots \\ y_1 L_1^{(m+n-2)} + y_2 L_2^{(m+n-2)} + \cdots + y_n L_n^{(m+n-2)} &= 0 \end{aligned} \tag{5.3}$$

where, $L_j^{(q)}(|\psi_1\rangle) = \begin{cases} \sum_{i=1}^m A_{ij}^{(q)} x_i & \text{if } 1 \le q \le k, \\ \sum_{i=1}^m B_{ij}^{(q-k)} \bar{x}_i & \text{if } k+1 \le q \le k+\ell = m+n-2. \end{cases}$

If there is a nonzero product vector $|\psi_1\rangle \otimes |\psi_2\rangle$, then the rank of the $(m+n-2) \times n$ matrix $\left(L_j^{(i)}\right)$ should be less than n. Hence, there is no doubt that we first have to study the system of the equations given by the $n \times n$ minors of the matrix $\left(L_j^{(i)}\right)$.

Let $\mathbf{a} = (a_1, \cdots, a_m)$ be a solution of the system of the equations given by the $n \times n$ minors of the matrix $\left(L_j^{(i)}\right)$, i.e. the matrix $\left(L_j^{(i)}(\mathbf{a})\right)$ has the rank less than n. Then there are two possibilities as follows:

(i) If the rank of the matrix $\left(L_j^{(i)}(\mathbf{a})\right)$ is exactly $n-1$, then the system of linear equations (5.3) in y_i has a unique nontrivial solution up to constant.

(ii) If the rank of the matrix $\left(L_j^{(i)}(\mathbf{a})\right)$ is less than $n-1$, then the system of linear equations (5.3) in y_i has infinitely many nontrivial solutions up to constant.

If the case (ii) happens for some $\mathbf{a} = (a_1, \cdots, a_m)$, then there are infinitely many nonzero product vectors $|\psi_1, \psi_2\rangle$ satisfying the condition (5.1). So, it is reasonable to focus only on the case where the rank of the matrix $\left(L_j^{(i)}(\mathbf{a})\right)$ is exactly $n-1$ for every solution $\mathbf{a}$ of the system of equations given by the $n \times n$ minors of the matrix $\left(L_j^{(i)}\right)$. In this case, we notice that the number of nonzero product vectors $|\psi_1\rangle \otimes |\psi_2\rangle$ satisfying the condition (5.1) is exactly the same as the number of common roots of the system of equations given by the $n \times n$ minors of the matrix $\left(L_j^{(i)}(\mathbf{a})\right)$. We note that if the matrix $\left(L_j^{(i)}(\mathbf{a})\right)$ has always rank n, then there is no nonzero product vector satisyfing the condition (5.1).

We first consider the particular case $\ell = 0$. In this case, the condition (5.1) in nothing but the condition

$$|\psi_1\rangle \otimes |\psi_2\rangle \in D$$

for subspaces D of $\mathbb{C}^m \otimes \mathbb{C}^n$ of codimension $m+n-2$. If we consider $|\psi_1\rangle \otimes |\psi_2\rangle$ as an element of the Segre variety $Seg(\mathbb{P}^{m-1} \times \mathbb{P}^{n-1})$, the condition (5.1) is nothing but the intersection of the Segre variety $Seg(\mathbb{P}^{m-1} \times \mathbb{P}^{n-1})$ and $m+n-2$ hyperplanes whose intersection is D, so the number of product vector $|\psi_1\rangle \otimes |\psi_2\rangle$ satisfying the condition (5.1) is less than or equal to the

degree of the Segre variety whenever it is finite and the equality holds for a generic choice of D.

Proposition 5.1.1. *Let* D *be a subspace of* $\mathbb{C}^m \otimes \mathbb{C}^n$ *with* $\dim D^\perp = m+n-2$. *Then*

(i) the number of nonzero product vectors in D *is less than or equal to*

$$\binom{m+n-2}{m-1}$$

whenever it is finite.

(ii) The equality holds for a generic choice of D.

This is exactly the particular case of Corollary 4.3.2 for $r = 1$, $n = 2$, $d_1 = m$ and $d_2 = n$. This result also mentioned in [WS08]. For the case $k = 0$, we can obtain the same result by symmetry. However, if $k \neq 0$ and $\ell \neq 0$, then we have to deal with a system of polynomial equations not in only complex variables, but in both complex variables and their conjugates. This causes many tricky situations to control equations. For instance, let us consider a single polynomial equation in z and $\bar{z}$

$$z^3 - \bar{z} = 0.$$

How many roots does this equation have? By a direct calculation, we get the exactly 5 solutions $z = 0, \pm 1, \pm i$. This means that the number of solutions does not obey the degree bound unlike the usual polynomial equation in z. Of course, it is also true that a system of equations in complex variables and their conjugates can violate the Bezout's theorem. Moreover, the equation $z\bar{z} - 1 = 0$ has infinitely many solutions, but the equation $z\bar{z} + 1 = 0$ has no solution. A series of examples show that it is very hard to control the number of common roots of a system of equations when we have to deal with both complex variables and their conjugates simultaneously.

5.2 Qubit-qunit case

In order to treat the system of equations (5.1) more in an elaborate way, let us particularly concentrate on the qubit-qunit case, i.e. the $\mathbb{C}^2 \otimes \mathbb{C}^n$ case. Then the rank condition on $\left(L_j^{(i)}\right)$ in the previous section turns into the condition that the rank of the $n \times n$ square matrix $\left(L_j^{(i)}\right)$ is greater than or equal to $n-1$. This is nothing but the condition that

$$\begin{aligned} &\textit{there is a nonvanishing } (n-1)\times(n-1) \textit{ minor of } \left(L_j^{(i)}\right) \\ &\textit{for every solution } \mathbf{a} \textit{ of } \det\left(L_j^{(i)}\right) = 0. \end{aligned} \tag{5.4}$$

We note that $\det(L_j^{(i)})$ is a bi-homogeneous polynomial of degree k in variables x_1, x_2 and of degree ℓ in variables $\bar{x_1}, \bar{x_2}$. Since we do not regard the case that both x_1 and x_2 are zero, we may assume $x_2 = 1$ without loss of generality, so $\det(L_j^{(i)})$ becomes a polynomial in x_1 and $\bar{x_1}$.

Now, we define the two polynomials P and Q determined by D and E as follows:

$$\begin{aligned} &P_{D,E}(z,w) := \text{the polynomial satisfying } P(x_1,\bar{x}_1) = \det(L_j^{(i)}), \\ &Q_{D,E}(z,w) := \text{the polynomial satisfying } Q(x_1,\bar{x}_1) = \overline{P(x_1,\bar{x}_1)}. \end{aligned} \tag{5.5}$$

Then we can state the main theorem of this section as follows.

Theorem 5.2.1. *Let D and E be subspaces of $\mathbb{C}^2 \otimes \mathbb{C}^n$ with $\dim D^\perp = k$ and $\dim E^\perp = l$. The polynomials $P_{D,E}$ and $Q_{D,E}$ are defined by (5.5). For the critical case $k+\ell = n$, the number of nonzero product vectors $|\psi_1\rangle \otimes |\psi_2\rangle$ satisfying the condition (5.1) is less than or equal to the mixed volume*

$$MV_2(New(P_{D,E}) \cup \{0\}, New(Q_{D,E}) \cup \{0\})$$

if the condition (5.4) is satisfied and the resultant $Res_w(P_{D,E}, Q_{D,E})$ is not identically zero.

Proof. From the discussion of the previous section, it is enough to estimate

the number of roots of the equation $P_{D,E}(z,\bar{z}) = 0$. For brevity, we write P and Q for $P_{D,E}$ and $Q_{D,E}$ respectively. Since the polynomial $Q(z,w)$ satisfies the condition $Q(z,\bar{z}) = \overline{P(z,\bar{z})}$, it is clear that if $(z,\bar{z})$ is a root of the equation $P(z,\bar{z}) = 0$, then so is the equation $Q(z,\bar{z}) = 0$. On the other hand, by Theorem 2.10.4, $P(z,w)$ and $Q(z,w)$ have no nontrivial common factor since the resultant $\mathrm{Res}_w(P,Q)$ is not identically zero. Over $\mathbb{C}$, this is equivalent to saying that the number of common roots in $\mathbb{C}^2$ is finite. By Theorem 2.9.7,

$$\begin{aligned}\left|\{\ z \in \mathbb{C} \mid P(z,\bar{z}) = 0\ \}\right| &= \left|\{\ z \in \mathbb{C} \mid P(z,\bar{z}) = Q(z,\bar{z}) = 0\ \}\right| \\ &\leq \left|\{\ (z,w) \in \mathbb{C}^2 \mid P(z,w) = Q(z,w) = 0\ \}\right| \\ &\leq MV_2(New(P) \cup \{0\}, New(Q) \cup \{0\}).\end{aligned}$$

Hence, the number of nonzero product vectors $|\psi_1\rangle \otimes |\psi_2\rangle$ satisfying the condition (5.1) is less than or equal to the mixed volume $MV_2(New(P_{D,E}) \cup \{0\}, New(Q_{D,E}) \cup \{0\})$.

□

We notice that it is essential to know how restrictive the condition that the condition (5.4) is satisfied and the resultant $\mathrm{Res}_w(P_{D,E}, Q_{D,E})$ is not identically zero is. The following proposition says that the condition satisfies for generic choices of D and E.

Proposition 5.2.2. *Let D and E be elements of the Grassmann varieties $\mathrm{Gr}(k, \mathbb{C}^2 \otimes \mathbb{C}^n)$ and $\mathrm{Gr}(\ell, \mathbb{C}^2 \otimes \mathbb{C}^n)$ respectively. Then there is a dense subset of $\mathrm{Gr}(k, \mathbb{C}^2 \otimes \mathbb{C}^n) \times \mathrm{Gr}(\ell, \mathbb{C}^2 \otimes \mathbb{C}^n)$ in which the condition (5.4) is satisfied and the resultant $\mathrm{Res}_w(P_{D,E}, Q_{D,E})$ is not identically zero.*

Proof. Since the polynomial $P_{D,E}$ is the polynomial of bidegree at most (k,ℓ), it can be regarded as an element of the projective space $\mathbb{P}^{(k+1)(\ell+1)-1}$ which is the projectivization of the set of all polynomials in two variables of bidegree at most (k,ℓ). We define a map

$$\begin{array}{rccc} \phi : \mathrm{Gr}(k, \mathbb{C}^2 \otimes \mathbb{C}^n) \times \mathrm{Gr}(\ell, \mathbb{C}^2 \otimes \mathbb{C}^n) & \longrightarrow & \mathbb{P}^{(k+1)(\ell+1)-1}. \\ (D,E) & \mapsto & P_{D,E} \end{array}$$

We claim that ϕ is well-defined and algebraic. For each pair $(D, E) \in \mathrm{Gr}(k, \mathbb{C}^2 \otimes \mathbb{C}^n) \times \mathrm{Gr}(\ell, \mathbb{C}^2 \otimes \mathbb{C}^n)$, we can write $D = \bigcap_{i=1}^{k} V_i^{\perp}$ and $E = \bigcap_{j=1}^{l} W_j^{\perp}$ for some vectors V_i, W_j in $\mathbb{C}^2 \otimes \mathbb{C}^n$. We denote the coordinates of V_i and W_j as

$$V_i = \left(A_{1,1}^{(i)}, \cdots, A_{1,n}^{(i)}, A_{2,1}^{(i)}, \cdots, A_{2,n}^{(i)}\right),$$
$$W_j = \left(B_{1,1}^{(j)}, \cdots, B_{1,n}^{(j)}, B_{2,1}^{(j)}, \cdots, B_{2,n}^{(j)}\right),$$

for $1 \leq i \leq k$, $1 \leq j \leq \ell$. Then the matrix $\left(L_j^{(i)}\right)$ is

$$\begin{pmatrix} A_{1,1}^{(1)} x_1 + A_{2,1}^{(1)} & \cdots & A_{1,n}^{(1)} x_1 + A_{2,n}^{(1)} \\ \vdots & & \vdots \\ A_{1,1}^{(k)} x_1 + A_{2,1}^{(k)} & \cdots & A_{1,n}^{(k)} x_1 + A_{2,n}^{(k)} \\ B_{1,1}^{(1)} \bar{x}_1 + B_{2,1}^{(1)} & \cdots & B_{1,n}^{(1)} \bar{x}_1 + B_{2,n}^{(1)} \\ \vdots & & \vdots \\ B_{1,1}^{(\ell)} \bar{x}_1 + B_{2,1}^{(\ell)} & \cdots & B_{1,n}^{(\ell)} \bar{x}_1 + B_{2,n}^{(\ell)} \end{pmatrix}.$$

Since $P_{D,E}(x_1, \bar{x}_1) = \det(L_j^{(i)})$, all the coefficients of the polynomial $P_{D,E}(z, w)$ are polynomials in $A_{r,s}^{(i)}$ and $B_{r,s}^{(j)}$, i.e. ϕ is algebraic if it is well-defined.

For another representations of $D = \bigcap_{i=1}^{k} (V_i')^{\perp}$ and $E = \bigcap_{k=1}^{\ell} (W_j')^{\perp}$, there are matrices $M_V \in \mathrm{GL}(k)$ and M_W in $\mathrm{GL}(\ell)$ such that

$$\begin{pmatrix} — & V_1' & — \\ & \vdots & \\ — & V_k' & — \end{pmatrix} = M_V \cdot \begin{pmatrix} — & V_1 & — \\ & \vdots & \\ — & V_k & — \end{pmatrix}, \qquad \begin{pmatrix} — & W_1' & — \\ & \vdots & \\ — & W_\ell' & — \end{pmatrix} = M_W \cdot \begin{pmatrix} — & W_1 & — \\ & \vdots & \\ — & W_\ell & — \end{pmatrix}.$$

Then we can easily check that the image of ϕ differs by multiplication of $\det(M_V)\det(M_W)$, i.e, it is unchanged as an element of the projective space. Hence, ϕ is well-defined.

We note that the resultant $\mathrm{Res}_w(P_{D,E}, Q_{D,E})$ is a polynomial in z whose coefficients are polynomials in the coefficients of $P_{D,E}$ and their conjugates. Hence, the locus that the resultant $\mathrm{Res}_w(P_{D,E}, Q_{D,E})$ is not identically zero

in the complex projective space $\mathbb{P}^{(k+1)(\ell+1)-1}$ is the complement of the finite union of the zero locus of real nonzero polynomial equations. This implies that the inverse $\phi^{-1}(\mathcal{W}')$ is also the complement of the finite union of the zero locus of real nonzero polynomial equations if it is nonempty.

We claim that $\phi^{-1}(\mathcal{W})$ is nonempty : We take

$$D = \bigcap_{j=1}^{k} \{z_{1j} + jz_{2j} = 0\}, \qquad E = \bigcap_{j=k+1}^{n} \{z_{1j} - jz_{2j} = 0\}.$$

Then

$$\begin{aligned} P_{D,E}(z,w) &= (z+1)(z+2)\cdots(z+k)(w-k-1)\cdots(w-n), \\ Q_{D,E}(z,w) &= (z-k-1)\cdots(z-n)(w+1)\cdots(w+k). \end{aligned}$$

We can readily verify that the resultant $\mathrm{Res}_w(P_{D,E}, Q_{D,E})$ of $P_{D,E}$ and $Q_{D,E}$ is $\prod_{j=1}^{k}\prod_{i=k+1}^{n}(i+j)(z-i)^k(z+j)^l$, which is not identically zero. Therefore, P should be located in $\mathcal{W}'$. Therefore, $\phi^{-1}(\mathcal{W}')$ is the complement of the finite union of the zero locus of real nonzero polynomial equations, so it is an dense subset of $\mathrm{Gr}(k, \mathbb{C}^2 \otimes \mathbb{C}^n) \times \mathrm{Gr}(\ell, \mathbb{C}^2 \otimes \mathbb{C}^n)$ for which the resultant $\mathrm{Res}_w(P_{D,E}, Q_{D,E})$ is not identically zero.

Moreover, the locus that the condition (5.4) is satisfied contains a Zariski open subset which is the union of the loci that the resultants of $P(z,w)$ and each $(n-1)\times(n-1)$ minors of $\left(L_j^{(i)}\right)$ is not identically zero. Therefore the locus that the condition (5.4) is satisfied and the resultant $\mathrm{Res}_w(P_{D,E}, Q_{D,E})$ is not identically zero is dense in $\mathrm{Gr}(k, \mathbb{C}^2 \otimes \mathbb{C}^n) \times \mathrm{Gr}(\ell, \mathbb{C}^2 \otimes \mathbb{C}^n)$. □

We note that the polynomial $P_{D,E}(z,w)$ and $Q_{D,E}(z,w)$ are bidegree at most (k,l) and (l,k) respectively. Hence, the mixed volume of $\mathrm{New}(P_{D,E}) \cup \{0\}$ and $\mathrm{New}(Q_{D,E}) \cup \{0\}$ is less than or equal to $(k+\ell)^2 - 2k\ell = k^2 + \ell^2$. See Figure 5.1. By Proposition 5.2.2, we obtain the following corollary.

Corollary 5.2.3. *Let* D *and* E *be subspaces of* $\mathbb{C}^2 \otimes \mathbb{C}^n$ *with* $\dim D^\perp = k$, $\dim E^\perp = l$. *Then the number of nonzero product vectors* $|\psi_1\rangle \otimes |\psi_2\rangle$ *satisfying the condition* (5.1) *is less than or equal to* $k^2 + \ell^2$ *for a generic choice of* D

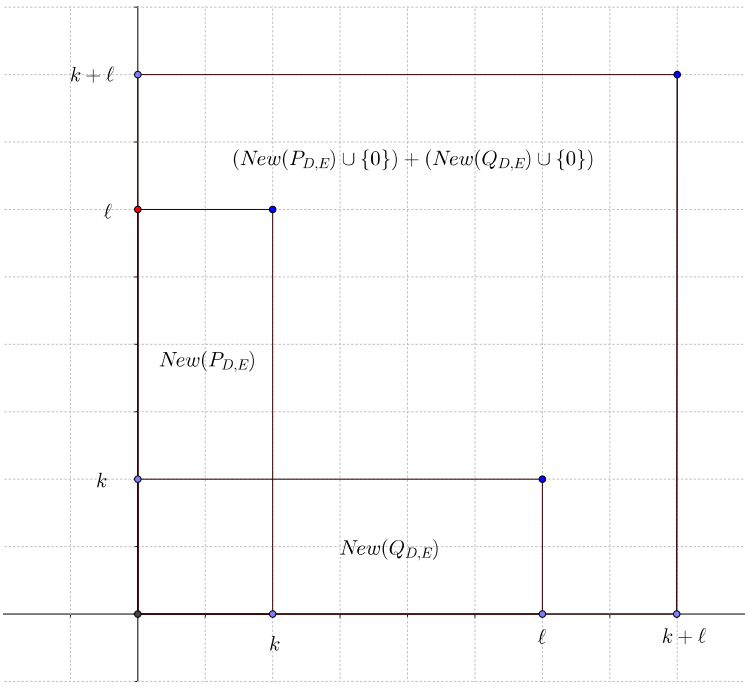

Figure 5.1: Newton polytopes of P and Q

and E.

By Proposition 5.1.1 and Corollary 5.2.3, we summarize the results as follows for some lower cases: Let D and E be subspaces $\mathbb{C}^2 \otimes \mathbb{C}^n$ with $\dim \mathsf{D}^\perp = k, \dim \mathsf{E}^\perp = \ell$.

- $\mathbb{C}^2 \otimes \mathbb{C}^2$ case : The number of product vectors $|\psi_1\rangle \otimes |\psi_2\rangle$ satisfying the condition (5.1) is

$$\begin{cases} \leq 2 & \text{whenever it is finite if } (k,l) = (2,0) \text{ or } (0,2), \\ \leq 2 & \text{for generic } \mathsf{D}, \mathsf{E} \text{ if } (k,l) = (1,1) \end{cases}$$

- $\mathbb{C}^2 \otimes \mathbb{C}^3$ case : The number of product vectors $|\psi_1\rangle \otimes |\psi_2\rangle$ satisfying

the condition (5.1) is

$$\begin{cases} \leq 3 & \text{whenever it is finite if } (k,l) = (3,0) \text{ or } (0,3), \\ \leq 5 & \text{for generic } D, E \text{ if } (k,l) = (2,1) \text{ or } (1,2) \end{cases}$$

- $\mathbb{C}^2 \otimes \mathbb{C}^4$ case : The number of product vectors $|\psi_1\rangle \otimes |\psi_2\rangle$ satisfying the condition (5.1) is

$$\begin{cases} \leq 4 & \text{whenever it is finite if } (k,l) = (4,0) \text{ or } (0,4) \\ \leq 10 & \text{for generic } D, E \text{ if } (k,l) = (3,1) \text{ or } (1,3) \\ \leq 8 & \text{for generic } D, E \text{ if } (k,l) = (2,2) \end{cases}$$

Kye [Kye13] described the conditions for which the number of product vectors is $0, 1, 2$ and ∞ explicitly in $\mathbb{C}^2 \otimes \mathbb{C}^2$ case. Ha and Kye [HK14] constructed an example in $\mathbb{C}^2 \otimes \mathbb{C}^3$ case in which there are exactly 5 product vectors for $(k,l) = (1,2)$ or $(2,1)$. Recently, they [HK13] also discovered examples in $\mathbb{C}^2 \otimes \mathbb{C}^4$ case in which there are exactly 10 product vectors for $(k,l) = (1,3)$ or $(3,1)$. These are strong evidences the upper bound $k^2 + l^2$ could be sharp.

Estimating the number of nonzero product vectors with (5.1) has some significant applications. For instance, it is relevant to the length $L(\rho)$ of a separable state ρ, which is the minimum number of product vectors required to represent the separable state ρ. It is known that any separable state ρ on $\mathbb{C}^m \otimes \mathbb{C}^n$ has length at most $(mn)^2$ [Hor97]. Since $L(\rho) \geq \operatorname{rank}(\rho)$ by definition, it is natural to ask if there is a separable state ρ on $\mathbb{C}^m \otimes \mathbb{C}^n$ with $L(\rho) > \operatorname{rank}(\rho)$. There are separable states ρ with $L(\rho) > \operatorname{rank}(\rho)$ [DTT00]. Furthermore, Chen and Đoković [CĐ13] proved that there are separable states ρ with $L(\rho) > mn$ whenever $(m-1)(n-1) > 2$ and conjectured that any separable state on $\mathbb{C}^2 \otimes \mathbb{C}^n$ has length not more than $2n$. However, soon after, examples of separable states ρ in $\mathbb{C}^2 \otimes \mathbb{C}^4$ whose length is 10 were discovered [HK13]. Note that Theorem 5.2.1 and Corollary 5.2.3 implies the following.

Corollary 5.2.4. *Let* D *and* E *be subspaces of* $\mathbb{C}^2 \otimes \mathbb{C}^n$ *such that the sum of the codimension of* D *and that of* E *is* n. *Let* $P_{D,E}$ *and* $Q_{D,E}$ *be polynomials given by* (5.5). *We assume that the resultant* $\mathrm{Res}_w(P_{D,E}, Q_{D,E})$ *is not identically zero and the condition* (5.4) *is satisfied. Then any separable state* ρ *on the Hilbert space* $\mathbb{C}^2 \otimes \mathbb{C}^n$ *satisfying* $\mathcal{R}(\rho) \subset D$ *and* $\mathcal{R}(\rho^\Gamma) \subset E$ *has length at most* $(\dim D^\perp)^2 + (\dim E^\perp)^2$.

In the next section, we give some examples of separable states ρ whose length are exactly $(\dim D^\perp)^2 + (\dim E^\perp)^2$. See Example 5.3.1 and 5.3.2.

5.3 Examples

The following is an example of the state ρ on $\mathbb{C}^2 \otimes \mathbb{C}^3$ whose length is 5 with $\dim \mathcal{R}(\rho)^\perp = 1$ and $\dim \mathcal{R}(\rho^\Gamma)^\perp = 2$. This realizes the upper bound in Corollary 5.2.4 as the sharp upper bound.

Example 5.3.1. [HK14] Let

$$D = \{(z_{ij}) \in \mathbb{C}^2 \otimes \mathbb{C}^3 \mid z_{13} - z_{21} = 0\},$$
$$E = \{(z_{ij}) \in \mathbb{C}^2 \otimes \mathbb{C}^3 \mid z_{12} - z_{21} = 0, z_{13} - z_{22} = 0\}.$$

Then the matrix $\left(L_j^{(i)}\right)$ given in the system of equations (5.3) is

$$\left(L_j^{(i)}\right) = \begin{pmatrix} -x_2 & 0 & x_1 \\ -\bar{x}_2 & \bar{x}_1 & 0 \\ 0 & -\bar{x}_2 & \bar{x}_1 \end{pmatrix}.$$

By the linear transformation $x_2 \mapsto x_2 + 2x_1$, the matrix $\left(L_j^{(i)}\right)$ turns into

$$\left(L_j^{(i)}\right) = \begin{pmatrix} -x_2 - 2x_1 & 0 & x_1 \\ -\bar{x}_2 - 2\bar{x}_1 & \bar{x}_1 & 0 \\ 0 & -\bar{x}_2 - 2\bar{x}_1 & \bar{x}_1 \end{pmatrix}.$$

The determinant of $\left(L_j^{(i)}\right)$ is $\det\left(L_j^{(i)}\right) = (\bar{x}_2 + 2\bar{x}_1)^2 x_1 - (x_2 + 2x_1)\bar{x}_1^2$. Since

$(x_1, x_2) = (1, 0)$ is not a solution of the equation $\det\left(L_j^{(i)}\right) = 0$, we may take $x_2 = 1$. Then the determinant $\det\left(L_j^{(i)}\right)$ turns into

$$(1 + 2\bar{x}_1)^2 x_1 - (1 + 2x_1)\bar{x}_1^2.$$

Let $L(i, j)$ be the 2×2 submatrix of L deleting the i-th row and the j-th column. Since at least one of the determinant of $L(1, 3)$ and $L(3, 1)$ is not zero, the rank of L must be 2. It means that the number of nonzero product vectors $|\psi_1\rangle \otimes |\psi_2\rangle$ satisfying the condition (5.1) is equal to the number of roots of $\det\left(L_j^{(i)}\right) = 0$.

In order to estimate the number of roots of $\det\left(L_j^{(i)}\right) = 0$, we take $P(z, w)$ and $Q(z, w)$ as (5.5). Then

$$\begin{aligned} P(z, w) &= (1 + 2w)^2 z - (1 + 2z)w^2, \\ Q(z, w) &= (1 + 2z)^2 w - (1 + 2w)z^2. \end{aligned}$$

The Newton polytope of P and Q are

$$\begin{aligned} New(P) &= \mathrm{Conv}(\{(1, 0), (0, 2), (1, 2)\}), \\ New(Q) &= \mathrm{Conv}(\{(2, 0), (0, 1), (2, 1)\}). \end{aligned}$$

Then

$$\begin{aligned} &New(P) \cup \{0\} = \mathrm{Conv}(\{(0, 0), (1, 0), (0, 2), (1, 2)\}), \\ &New(Q) \cup \{0\} = \mathrm{Conv}(\{(0, 0), (2, 0), (0, 1), (2, 1)\}), \\ &New(P) \cup \{0\} + New(Q) \cup \{0\} = \mathrm{Conv}(\{(0, 0), (3, 0), (0, 3), (3, 3)\}). \end{aligned}$$

Hence, the mixed volume $MV_2(New(P) \cup \{0\}, New(Q) \cup \{0\})$ is

$$\begin{aligned} MV_2(New(P) \cup \{0\}, New(Q) \cup \{0\}) &= \mathrm{Vol}_2(New(P) \cup \{0\} + New(Q) \cup \{0\}) \\ &\quad - \mathrm{Vol}_2(New(P) \cup \{0\}) - \mathrm{Vol}_2(New(Q) \cup \{0\}) \\ &= 9 - 2 - 2 = 5. \end{aligned}$$

By Theorem 2.9.7, the number of common roots of P and Q in $\mathbb{C}^2$ is less than or equal to 5. As a corollary, we can say that any separable state ρ with $\mathcal{R}(\rho) \subset D$ and $\mathcal{R}(\rho^\Gamma) \subset E$ has length at most 5. In fact, there is an explicit example of a separable state of length 5 with $\mathcal{R}(\rho) = D$ and $\mathcal{R}(\rho^\Gamma) = E$. Let ρ be a separable state

$$\rho = \sum_{i=0}^{5} |\psi_i\rangle\langle\psi_i|,$$

where $|\psi_i\rangle$ are defined as follows:

$$\begin{aligned} |\psi_i\rangle &= (1, \omega^i)^t \otimes (1, \omega^i, \omega^{2i})^t \qquad \text{for } i = 0, 1, 2, \\ |\psi_3\rangle &= (0, 1)^t \otimes (0, 0, 1)^t, \quad |\psi_4\rangle = (1, 0)^t \otimes (1, 0, 0)^t. \end{aligned}$$

We can easily check that the range $\mathcal{R}(\rho)$ of ρ is D and the range $\mathcal{R}(\rho^\Gamma)$ of its partial transpose ρ^Γ is E.

We also give an example of the state ρ on $\mathbb{C}^2 \otimes \mathbb{C}^4$ whose length is 10 with $\dim \mathcal{R}(\rho)^\perp = 3$ and $\dim \mathcal{R}(\rho^\Gamma)^\perp = 1$. This realizes the upper bound in Corollary 5.2.4 as the sharp upper bound.

Example 5.3.2. [HK13] Let a and b be real numbers with the relation $0 < b < 4a^3/27$. Then the equation $r^3 - ar^2 + b = 0$ has two distinct positive real roots r_1 and r_2. Let r_3 be the only positive real root of $r^3 + ar^2 - b = 0$. Note that r_1, r_2 and r_3 are distinct from each other. We take the complex numbers α_i as follows:

$$\begin{aligned} &\alpha_1 = r_1, \quad \alpha_2 = r_1\omega, \quad \alpha_3 = r_1\omega^2, \\ &\alpha_4 = r_2, \quad \alpha_5 = r_2\omega, \quad \alpha_6 = r_2\omega^2, \\ &\alpha_7 = -r_3, \quad \alpha_8 = -r_3\omega, \quad \alpha_9 = -r_3\omega^2, \end{aligned}$$

where ω is the third root of unity. Now, we let

$$|\psi_0\rangle = (0, 1)^t \otimes (0, 0, 0, 1)^t, \quad |\psi_i\rangle = (1, \alpha_i)^t \otimes (1, \alpha_i, \alpha_i^2, \alpha_i^3)^t \quad \text{for } 1 \le i \le 9.$$

and take a separable state ρ as

$$\rho = \sum_{i=0}^{9} |\psi_i\rangle\langle\psi_i|.$$

Then its range $\mathcal{R}(\rho)$ and the range $\mathcal{R}(\rho^\Gamma)$ of its partial transpose ρ^Γ are

$$\mathcal{R}(\rho) = D = \{(z_{ij}) \in \mathbb{C}^2 \otimes \mathbb{C}^4 \mid z_{12} - z_{21} = 0, z_{13} - z_{22} = 0, z_{14} - z_{23} = 0\},$$
$$\mathcal{R}(\rho^\Gamma) = E = \{(z_{ij}) \in \mathbb{C}^2 \otimes \mathbb{C}^4 \mid bz_{11} + z_{14} - az_{22} = 0\}.$$

Then the matrix $\left(L_j^{(i)}\right)$ given in the system of equations (5.3) is

$$\left(L_j^{(i)}\right) = \begin{pmatrix} -x_2 & x_1 & 0 & 0 \\ 0 & -x_2 & x_1 & 0 \\ 0 & 0 & -x_2 & x_1 \\ b\bar{x}_1 & -a\bar{x}_2 & 0 & \bar{x}_1 \end{pmatrix}.$$

The determinant of $\left(L_j^{(i)}\right)$ is $ax_1^2x_2\bar{x}_2 - bx_1^3\bar{x}_1 - x_2^3\bar{x}_1$. Since $(x_1, x_2) = (1, 0)$ is not a root of the equation $\det\left(L_j^{(i)}\right) = 0$, we may assume $x_2 = 1$. Then the determinant $\det\left(L_j^{(i)}\right)$ turns into

$$ax_1^2 - bx_1^3\bar{x}_1 - \bar{x}_1.$$

Now, we follow the process in Example 5.3.1 in the same way. Since the 3×3 minor of $\left(L_j^{(i)}\right)$ consisting of first 3 rows and first 3 columns is not zero, $\left(L_j^{(i)}\right)$ has rank 3 for every x_1. It means that the number of nonzero product vectors $|\psi_1\rangle \otimes |\psi_2\rangle$ satisfying the condition (5.1) is equal to the number of roots of $\det\left(L_j^{(i)}\right) = 0$.

In order to estimate the number of roots of $\det\left(L_j^{(i)}\right) = 0$, we take

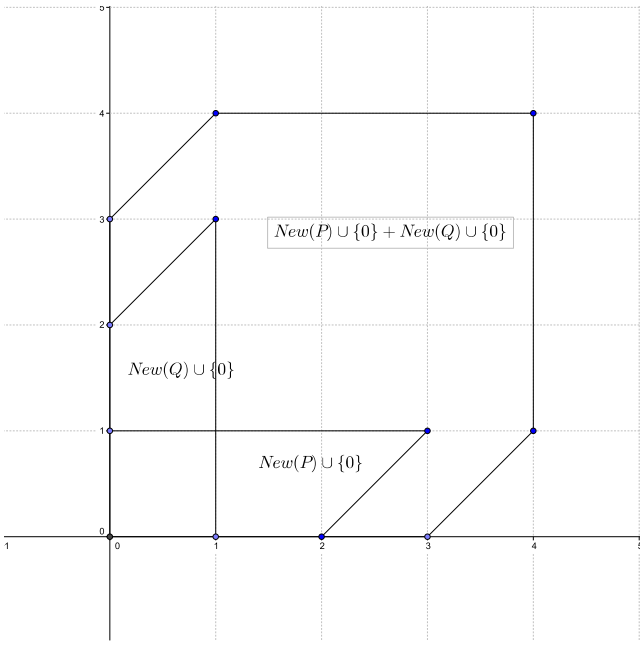

Figure 5.2: Example: 5.3.2

$P(z,w)$ and $Q(z,w)$ as (5.5). Then

$$P(z,w) = -bz^3w + az^2 - w,$$
$$Q(z,w) = -bw^3z + aw^2 - z.$$

The Newton polytope of P and Q are

$$New(P) = \mathrm{Conv}(\{(3,1),(2,0),(0,1)\}),$$
$$New(Q) = \mathrm{Conv}(\{(1,3),(0,2),(1,0)\}).$$

Then

$$New(P) \cup \{0\} = \mathrm{Conv}(\{(0,0),(3,1),(2,0),(0,1)\}),$$
$$New(Q) \cup \{0\} = \mathrm{Conv}(\{(0,0),(1,3),(0,2),(1,0)\}),$$
$$New(P) \cup \{0\} + New(Q) \cup \{0\} = \mathrm{Conv}(\{(0,0),(3,0),(4,1),(0,3),(1,4),(4,4)\}).$$

Hence, the mixed volume $MV_2(New(P) \cup \{0\}, New(Q) \cup \{0\})$ is

$$\begin{aligned} MV_2(New(P) \cup \{0\}, New(Q) \cup \{0\}) &= Vol_2(New(P) \cup \{0\} + New(Q) \cup \{0\}) \\ &\quad - Vol_2(New(P) \cup \{0\}) - Vol_2(New(Q) \cup \{0\}) \\ &= 15 - \frac{5}{2} - \frac{5}{2} = 10. \end{aligned}$$

By Theorem 2.9.7, the number of common roots of P and Q in $\mathbb{C}^2$ is less than or equal to 10. As a corollary, we can say that any separable state ρ with $\mathcal{R}(\rho) \subset D$ and $\mathcal{R}(\rho^\Gamma) \subset E$ has length at most 10. We put again emphasis on the separable state ρ defined above has length exactly 10 and satisfies $\mathcal{R}(\rho) = D$ and $\mathcal{R}(\rho^\Gamma) = E$.

Now, we consider another application of Theorem 5.2.1. By the range criterion, if the number of nonzero product vectors $|\psi_1\rangle \otimes |\psi_2\rangle$ satisfying the condition (5.1) is less than either the dimension of D or that of E, then all the PPT states ρ satisfying $\mathcal{R}(\rho) \subset D$ and $\mathcal{R}(\rho^\Gamma) \subset E$ are entangled. Unfortunately, the number $k^2 + \ell^2$ in Corollary 5.2.3 is bigger than both of the dimension of D and that of E in general. However, for some particular D and E, we can show that the mixed volume $MV_2(New(P) \cup \{0\}, New(Q) \cup \{0\})$ is less than either the dimension of D or that of E. The following example appears in [Hor97]. We can check why the PPT state given in [Hor97] can not be separable more systematically by means of the discussion above.

Example 5.3.3. Let ρ be a state on $\mathbb{C}^2 \otimes \mathbb{C}^4$ given as follows:

$$\rho = \begin{pmatrix} \frac{1}{3} & 0 & 0 & 0 & 0 & \frac{1}{3} & 0 & 0 \\ 0 & \frac{1}{3} & 0 & 0 & 0 & 0 & \frac{1}{3} & 0 \\ 0 & 0 & \frac{1}{3} & 0 & 0 & 0 & 0 & \frac{1}{3} \\ 0 & 0 & 0 & \frac{1}{3} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{2}{3} & 0 & 0 & \frac{\sqrt{2}}{3} \\ \frac{1}{3} & 0 & 0 & 0 & 0 & \frac{1}{3} & 0 & 0 \\ 0 & \frac{1}{3} & 0 & 0 & 0 & 0 & \frac{1}{3} & 0 \\ 0 & 0 & \frac{1}{3} & 0 & \frac{\sqrt{2}}{3} & 0 & 0 & \frac{2}{3} \end{pmatrix}.$$

Then its range $\mathcal{R}(\rho)$ and the range $\mathcal{R}(\rho^\Gamma)$ of its partial transpose ρ^Γ are

$$\mathcal{R}(\rho) = \left\{ (z_{ij}) \in \mathbb{C}^2 \otimes \mathbb{C}^4 \;\middle|\; z_{11} - z_{12} = 0,\ z_{12} - z_{23} = 0,\ z_{13} + \frac{1}{\sqrt{2}} z_{21} - z_{24} = 0 \right\}$$

and

$$\mathcal{R}(\rho^\Gamma) = \left\{ (z_{ij}) \in \mathbb{C}^2 \otimes \mathbb{C}^4 \;\middle|\; z_{13} - z_{22} = 0,\ z_{14} - z_{23} = 0,\ z_{12} + \frac{1}{\sqrt{2}} z_{24} - z_{21} = 0 \right\}.$$

Let D and E be subspaces of $\mathbb{C}^2 \otimes \mathbb{C}^4$ taken as follows:

$$D = \left\{ (z_{ij}) \in \mathbb{C}^2 \otimes \mathbb{C}^4 \;\middle|\; z_{11} - z_{12} = 0,\ z_{13} + \frac{1}{\sqrt{2}} z_{21} - z_{24} = 0 \right\},$$
$$E = \left\{ (z_{ij}) \in \mathbb{C}^2 \otimes \mathbb{C}^4 \;\middle|\; z_{14} - z_{23} = 0,\ z_{12} + \frac{1}{\sqrt{2}} z_{24} - z_{21} = 0 \right\}.$$

It is clear that $\mathcal{R}(\rho) \subset D$ and $\mathcal{R}(\rho^\Gamma) \subset E$. Now, we claim that there are at most 4 nonzero product vectors satisfying the condition (5.1). If this claim is true, then ρ can not be a separable state by the range criterion.

In this case, the matrix $\left(L_j^{(i)}\right)$ given in the system of equations (5.3) is

$$\left(L_j^{(i)}\right) = \begin{pmatrix} x_1 & -x_2 & 0 & 0 \\ \frac{1}{\sqrt{2}} x_1 & 0 & x_1 & -x_2 \\ 0 & 0 & -\bar{x}_2 & \bar{x}_1 \\ -\bar{x}_2 & \bar{x}_1 & 0 & \frac{1}{\sqrt{2}} \bar{x}_2 \end{pmatrix}.$$

Its determinant is $\det\left(L_j^{(i)}\right) = 2x_1x_2\bar{x}_1\bar{x}_2 - x_1^2\bar{x}_1^2 + \frac{1}{2}x_1x_2\bar{x}_2^2 - x_2^2\bar{x}_2^2$. Since $(x_1, x_2) = (1, 0)$ is not a root of the equation $\det\left(L_j^{(i)}\right) = 0$, we may assume $x_2 = 1$. Then the determinant $\det\left(L_j^{(i)}\right)$ turns into

$$-x_1^2\bar{x}_1^2 + 2x_1\bar{x}_1 + \frac{1}{2}x_1 - 1.$$

Since $x_1 = 0$ is not a root of $\det\left(L_j^{(i)}\right) = 0$, the submatrix of $\left(L_j^{(i)}\right)$ consist-

ing of the first 3 rows and the last 3 columns has rank 3 for every root of $\det\left(L_j^{(i)}\right) = 0$. It means that the number of nonzero product vectors satisfying the condition (5.1) is equal to the number of roots of $\det\left(L_j^{(i)}\right) = 0$.

In order to estimate the number of roots of $\det\left(L_j^{(i)}\right) = 0$, we take $P(z,w)$ and $Q(z,w)$ as (5.5). Then

$$P(z,w) = -z^2w^2 + 2zw + \frac{1}{2}z - 1,$$
$$Q(z,w) = -z^2w^2 + 2zw + \frac{1}{2}w - 1.$$

The Newton polytope of P and Q are

$$New(P) = \mathrm{Conv}(\{(0,0),(1,0),(2,2)\}),$$
$$New(Q) = \mathrm{Conv}(\{(0,0),(0,1),(2,2)\}).$$

Then

$$New(P)\cup\{0\} = New(P), \qquad New(Q)\cup\{0\} = New(Q),$$
$$New(P)\cup\{0\} + New(Q)\cup\{0\} = \mathrm{Conv}(\{(0,0),(1,0),(0,1),(3,2),(2,3),(4,4)\}).$$

Hence, the mixed volume $MV_2(New(P)\cup\{0\}, New(Q)\cup\{0\})$ is

$$\begin{aligned} MV_2(New(P)\cup\{0\}, New(Q)\cup\{0\}) &= \mathrm{Vol}_2(New(P)\cup\{0\} + New(Q)\cup\{0\}) \\ &\quad - \mathrm{Vol}_2(New(P)\cup\{0\}) - \mathrm{Vol}_2(New(Q)\cup\{0\}) \\ &= 6 - 1 - 1 = 4. \end{aligned}$$

By Theorem 2.9.7, the number of common roots of P and Q in $\mathbb{C}^2$ is less than or equal to 4. It implies that the number of product vectors $|\psi_1\rangle\otimes|\psi_2\rangle$ satisfying the condition (5.1) is at most 4, so they never span the the range $\mathcal{R}(\rho)$ because the dimension of $\mathcal{R}(\rho)$ is 5. By the range criterion, the state ρ is an entangled state. Moreover, we can say that any separable state ρ with $\mathcal{R}(\rho)\subset D$ and $\mathcal{R}(\rho^\Gamma)\subset E$ has length at most 4.

Let us consider another example for the $\mathbb{C}^2\otimes\mathbb{C}^4$ case.

Example 5.3.4. Let

$$D = \left\{ (z_{ij}) \in \mathbb{C}^2 \otimes \mathbb{C}^4 \;\middle|\; \begin{array}{c} z_{11} - z_{12} + 3z_{13} - 3z_{14} + 2z_{21} + (1+i)z_{22} = 0, \\ (-2+3i)z_{11} + 3z_{14} + z_{21} + 2z_{22} + (7-i)z_{23} - z_{24} = 0 \end{array} \right\}$$

and

$$E = \left\{ (z_{ij}) \in \mathbb{C}^2 \otimes \mathbb{C}^4 \;\middle|\; \begin{array}{c} 11z_{11} + 3z_{12} + z_{13} - 2z_{23} = 0, \\ (13-39i)z_{21} - (33-9i)z_{24} = 0 \end{array} \right\}.$$

We claim that for such D and E, there are at most 4 nonzero product vectors satisfying the condition (5.1). If this claim is true, then ρ can not be a separable state by the range criterion.

In this case, the matrix $\left(L_j^{(i)}\right)$ given in the system of equations (5.3) is

$$\left(L_j^{(i)}\right) = \begin{pmatrix} x_1 + 2x_2 & -x_1 + (1+i)x_2 & 3x_1 & -3x_1 \\ (-2+3i)x_1 + x_2 & 2x_2 & (7-i)x_2 & 3x_1 - x_2 \\ 11\bar{x}_1 & 3\bar{x}_1 & \bar{x}_1 - 2\bar{x}_2 & 0 \\ (13-39i)\bar{x}_2 & 0 & 0 & (-33+9i)\bar{x}_2 \end{pmatrix}.$$

Since $(x_1, x_2) = (1, 0)$ is not a root of the equation $\det\left(L_j^{(i)}\right) = 0$, we may assume $x_2 = 1$. Then the determinant $\det\left(L_j^{(i)}\right)$ turns into

$$(4630 + 120i)x_1^2\bar{x}_1^2 + (16 + 492i)x_1 - (2308 + 1876i)\bar{x}_1 + (284 - 172i).$$

Consider the 3×3 minor of last 3 rows and first 3 columns of the matrix $\left(L_j^{(i)}\right)$. It is $(13-39i)((-19+3i)\bar{x}-4)$. Since $x = -4/(19+3i)$ is not a root of the equation $\det\left(L_j^{(i)}\right) = 0$, all the roots of $\det\left(L_j^{(i)}\right) = 0$ make the rank of M to be 3. It means that the number of nonzero product vectors satisfying the condition (5.1) is equal to the number of roots of $\det\left(L_j^{(i)}\right) = 0$.

In order to estimate the number of roots of $\det\left(L_j^{(i)}\right) = 0$, we take $P(z, w)$ and $Q(z, w)$ as (5.5). Then

$$P(z, w) = (4630 + 120i)z^2w^2 + (16 + 492i)z - (2308 + 1876i)w + (284 - 172i),$$
$$Q(z, w) = (4630 - 120i)z^2w^2 - (2308 - 1876i)z + (16 - 492i)w + (284 + 172i).$$

The Newton polytope of P and Q are

$$New(P) = New(Q) = \mathrm{Conv}(\{(0,0),(1,0),(0,1),(2,2)\}),$$

Then

$$\begin{aligned} &New(P) \cup \{0\} = New(P), \qquad New(Q) \cup \{0\} = New(Q), \\ &New(P) \cup \{0\} + New(Q) \cup \{0\} = \mathrm{Conv}(\{(0,0),(2,0),(0,2),(4,4)\}). \end{aligned}$$

Hence, the mixed volume $MV_2(New(P) \cup \{0\}, New(Q) \cup \{0\})$ is

$$\begin{aligned} MV_2(New(P) \cup \{0\}, New(Q) \cup \{0\}) &= \mathrm{Vol}_2(New(P) \cup \{0\} + New(Q) \cup \{0\}) \\ &\quad - \mathrm{Vol}_2(New(P) \cup \{0\}) - \mathrm{Vol}_2(New(Q) \cup \{0\}) \\ &= 8 - 2 - 2 = 4. \end{aligned}$$

By Theorem 2.9.7, the number of common roots of P and Q in $\mathbb{C}^2$ is less than or equal to 4. It implies that the number of product vectors $|\psi_1\rangle \otimes |\psi_2\rangle$ satisfying the condition (5.1) is at most 4, any separable state ρ with $\mathcal{R}(\rho) \subset D$ and $\mathcal{R}(\rho^\Gamma) \subset E$ has length at most 4.

Chapter 6

Classification of Entangled States

Let us consider the set of pure separable states in a composite quantum system $\mathcal{H} = \bigotimes_{i=1}^{n} \mathcal{H}_i$. It is nothing but the Segre variety $\mathsf{Seg}(\prod_{i=1}^{n} \mathbb{P}(\mathcal{H}_i))$ in $\mathbb{P}(\mathcal{H})$, which is invariant under the action of a group of local invertible operations, i.e. the natural G-action on $\mathcal{H}$ for some subgroup G of $\prod_{i=1}^{n} \mathrm{GL}(\mathcal{H}_i)$. This means that an entanglement state can not be obtained from a separable state using only local manipulations of the subsystems. In this chapter, we only deal with the case $\mathsf{G} = \prod_{i=1}^{n} \mathrm{GL}(\mathcal{H}_i)$. Even though it is the coarser classification of the states, we only know few cases. For the case $\mathsf{G}' = \prod_{i=1}^{n} \mathrm{GL}(\mathcal{H}_i)$, any two given two separable states can be converted into each other because $\prod_{i=1}^{n} \mathbb{P}(\mathcal{H}_i)$ is a homogeneous G-space. However, we can not expect in general that any two entangled states can be linked via only local operations since the set of pure entangled states is much bigger than the separable one. Therefore, it is natural to ask the following question: If given two states can be converted into each other via only local invertible operations, we say that they are equivalent. Then

- How many inequivalent entangled states are there?
- Can we classify all the states up to equivalence completely?
- Can we determine whether any two given states are equivalent?

Clearly, these questions depend on the choice of a group of local invertible operations G.

6.1 Bipartite cases

Let $X = \mathbb{C}^m \otimes \mathbb{C}^n$ be a tensor product of finite dimensional vector spaces. The group $G = \mathrm{GL}(m) \times \mathrm{GL}(n)$ naturally acts on X via

$$(A, B) \cdot (\mathbf{x} \otimes \mathbf{y}) = A\mathbf{x} \otimes B\mathbf{y}$$

for $\mathbf{x} \in \mathbb{C}^m$, $\mathbf{y} \in \mathbb{C}^n$, $A \in \mathrm{GL}(m)$, $B \in \mathrm{GL}(n)$. The vector space $X = \mathbb{C}^m \otimes \mathbb{C}^n$ can be considered as the set $\mathfrak{M}_{m,n}$ of all $m \times n$ matrices via $\sum_i \mathbf{x}_i \otimes \mathbf{y}_i \mapsto \sum_i \mathbf{x}_i \mathbf{y}_i^t$. Then the G-action on $\mathfrak{M}_{m,n}$ is given by

$$(A, B) \cdot (\sum_i \mathbf{x}_i \mathbf{y}_i^t) = A \, (\sum_i \mathbf{x}_i \mathbf{y}_i^t) \, B^t.$$

Since an action of an invertible matrix can be expressed as a composition of elementary operations and nonzero scalar multiples of rows or columns, there always $A \in \mathrm{GL}(m)$ and $B \in \mathrm{GL}(n)$ such that the matrix $A \cdot (\sum_i \mathbf{x}_i \mathbf{y}_i^t) \cdot B^t$ can be put into the following form:

$$A \cdot (\sum_i \mathbf{x}_i \mathbf{y}_i^t) \cdot B^t = \left(\begin{array}{c|c} I_r & O \\ \hline O & O \end{array} \right),$$

where r is the rank of the $m \times n$ matrix $\sum_i \mathbf{x}_i \mathbf{y}_i^t$ and I_r is the $r \times r$ identity matrix. Hence, all the G-orbits are given by

$$O_r = \{ \text{ rank } r \text{ tensors in } \mathbb{C}^m \otimes \mathbb{C}^n \}$$

for $0 \leq r \leq \min(m, n)$, so if we would like to determine which orbit a given state on $\mathbb{C}^m \otimes \mathbb{C}^n$ belongs to, we only need to check that the rank of the state. We note that O_1 is exactly the set of all separable states and O_r is the set of entangled states whose ranks are equal to r for $2 \leq r \leq \min(m, n)$. Moreover, the Zariski closure of the orbit

$$\overline{O_r} = \{ \text{ rank } \leq r \text{ tensors in } \mathbb{P}(\mathbb{C}^m \otimes \mathbb{C}^n) \} = \mathbb{P}(\bigcup_{k=1}^{r} O_k)$$

is a closed subvariety of $\mathbb{P}(\mathbb{C}^m \otimes \mathbb{C}^n)$ for every r, which is exactly the secant variety $\sigma_r(\mathsf{Seg}(\mathbb{P}^{m-1} \times \mathbb{P}^{n-1}))$. Therefore, there is a stratification of $\mathbb{P}(\mathbb{C}^m \otimes \mathbb{C}^n)$ given by the orbit closures:

$$O_1 = \overline{O_1} \subset \overline{O_2} \subset \cdots \subset \overline{O_{\min(m,n)}} = \mathbb{P}(\mathbb{C}^m \otimes \mathbb{C}^n).$$

6.2 Three qubit case

The tripartite cases are more complicated than the bipartite cases. For instance, if we consider the three qubit case, i.e. $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ acted on by $G = \mathrm{GL}(2) \times \mathrm{GL}(2) \times \mathrm{GL}(2)$, then the orbit of $|100\rangle + |111\rangle$ and that of $|001\rangle + |111\rangle$ are different even though they have the same rank 2. Moreover, there are many cases for which infinitely many G-orbits exist.

Lemma 6.2.1. *Let* $X = \mathbb{C}^\ell \otimes \mathbb{C}^m \otimes \mathbb{C}^n$. *The group* $G = \mathrm{GL}(\ell) \times \mathrm{GL}(m) \times \mathrm{GL}(n)$ *acts on* X *via*

$$(A, B, C) \cdot \mathbf{x} \otimes \mathbf{y} \otimes \mathbf{z} = A\mathbf{x} \otimes B\mathbf{y} \otimes C\mathbf{z}.$$

If $\ell mn > \ell^2 + m^2 + n^2 - 2$, *then there are infinitely many* G*-orbits.*

Proof. The proof is easy. We note that if any two orbits differ by multiple of nonzero constant, they belong to the same G-orbit. Hence, the problem is equivalent that the group $G' = \mathrm{SL}(\ell) \times \mathrm{SL}(m) \times \mathrm{SL}(n)$ acts on the projective space $\mathbb{P}(\mathbb{C}^\ell \otimes \mathbb{C}^m \otimes \mathbb{C}^n)$. Since the dimension of G' and that of $\mathbb{P}(\mathbb{C}^\ell \otimes \mathbb{C}^m \otimes \mathbb{C}^n)$ are $\ell^2 + m^2 + n^2 - 3$ and $\ell mn - 1$ respectively, the result is clear. □

The condition $\ell mn \leq \ell^2+m^2+n^2-2$ is a minimal necessary condition for the number of the G-orbits to be finite. Of course, this may not be sufficient. As we will see, the case $\ell = 2, m = n = 4$ has infinitely many G-orbits even if $\ell mn < \ell^2 + m^2 + n^2 - 2$.

We assume that $2 \leq \ell \leq m \leq n$ without loss of generality. In order to analyze the case $\ell = 2$, we introduce a useful normal form of a pencil of matrices.

Theorem 6.2.2 (Kronecker normal form)**.** *[Gan60, Chapter XII] Let M_1 and M_2 be two $m \times n$ complex matrices. Let us consider a pencil of matrices*

$$M_{[s:t]} := sM_1 + tM_2 \qquad \textit{for } [s:t] \in \mathbb{P}^1.$$

Then there are matrices $A \in \mathrm{GL}(m)$ and $B \in \mathrm{GL}(n)$ such that the pencil of matrices $A \cdot M_{[s:t]} \cdot B$ have the following form:

$$\begin{pmatrix} L_{i_1} & & & & & & & & \\ & \ddots & & & & & & & \\ & & L_{\beta_p} & & & & & & \\ & & & L^t_{j_1} & & & & & \\ & & & & \ddots & & & & \\ & & & & & L^t_{j_q} & & & \\ & & & & & & J_{\lambda_1,k_1} & & \\ & & & & & & & \ddots & \\ & & & & & & & & J_{\lambda_d,k_d} \\ & & & & & & & & & 0 \end{pmatrix},$$

where L_i is a $i \times (i+1)$ matrix given by

$$L_i = \begin{pmatrix} s & t & & \\ & s & t & \\ & & \ddots & \ddots \\ & & & s & t \end{pmatrix}$$

and $J_{\lambda,k}$ *is a* $k \times k$ *matrix given by*

$$J_{\lambda,k} = \begin{pmatrix} s+t\lambda & t & & \\ & \ddots & \ddots & \\ & & s+t\lambda & t \\ & & & s+t\lambda \end{pmatrix}.$$

Let us first consider the $m = n = 2$ case. All the possible Kronecker normal forms are the following:

$$N_1 = \begin{pmatrix} s & t \\ 0 & 0 \end{pmatrix}, \qquad N_2 = \begin{pmatrix} s & 0 \\ t & 0 \end{pmatrix},$$
$$N_3 = \begin{pmatrix} s+\lambda t & t \\ 0 & s+\lambda t \end{pmatrix}, \qquad N_4 = \begin{pmatrix} s+\lambda_1 t & 0 \\ 0 & s+\lambda_2 t \end{pmatrix},$$

for $\lambda, \lambda_1, \lambda_2 \in \mathbb{C}$ and $\lambda_1 \neq \lambda_2$. Moreover, N_3 and N_4 can be transformed into the following simpler form under appropriate $\mathrm{GL}(2) \times \mathrm{GL}(2)$-actions:

$$N_3' = \begin{pmatrix} s & t \\ 0 & s \end{pmatrix}, \quad N_4' = \begin{pmatrix} s & 0 \\ 0 & t \end{pmatrix},$$

We note that all the N_1, N_2, N_3' and N_4' depend only on the variables s and t, i.e. the possible pencils of 2×2 matrices are exactly N_1, N_2, N_3' and N_4' up to a $\mathrm{GL}(2) \times \mathrm{GL}(2)$-action. This observation gives us the following.

Theorem 6.2.3 (Three qubit case)**.** *[HLT12, BL13] Let* $X = \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ *be the vector space acted on by the group* $G = \mathrm{GL}(2) \times \mathrm{GL}(2) \times \mathrm{GL}(2)$*. Then there are exactly* 6 G*-orbits as follows:*

$$O_1 := G \cdot |000\rangle, \qquad O_2 := G \cdot (|101\rangle + |110\rangle),$$
$$O_3 := G \cdot (|110\rangle + |011\rangle), \qquad O_4 := G \cdot (|101\rangle + |011\rangle),$$
$$O_5 := G \cdot (|110\rangle + |101\rangle + |011\rangle), \quad O_6 := G \cdot (|000\rangle + |111\rangle).$$

Proof. Let $\mathbf{t}$ be an element of $V_1 \otimes V_2 \otimes V_3$, where $V_1 = V_2 = V_3 = \mathbb{C}^2$. The tensor $\mathbf{t}$ can be regarded as a linear map $\mathbf{t}_{V_1} : V_1^* \longrightarrow V_2 \otimes V_3$. If the

dimension of the image $\mathbf{t}_{V_1}(V_1^*)$ is zero, then the tensor $\mathbf{t}$ itself should be zero. If the dimension of the image $\mathbf{t}_{V_1}(V_1^*)$ is one, i.e. $\mathbf{t}_{V_1}(V_1^*)$ is spanned by a vector $\mathbf{v}$ in $V_2 \otimes V_3$, then $\mathbf{v}$ has one of the following form by the discussion in the bipartite cases:

$$|00\rangle = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad |00\rangle + |11\rangle = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Let us consider the second case. Since $\mathbf{t}_{V_1}(V_1^*)$ is spanned by the vector $|00\rangle + |11\rangle$, we can write the images of $\langle 0|$ and $\langle 1|$ under the map $\mathbf{t}_{V_1}$ as $\alpha(|00\rangle + |11\rangle)$ and $\beta(|00\rangle + |11\rangle)$ for some $\alpha, \beta \in \mathbb{C}$ respectively. Then $\mathbf{t}$ should be $(\alpha|0\rangle + \beta|1\rangle) \otimes (|00\rangle + |11\rangle)$. By an appropriate G-action on $\mathbf{t}$, $\mathbf{t}$ can be put into the simpler form $|101\rangle + |110\rangle$. In the same way, for the first case, $\mathbf{t}$ can be transformed into the form $|000\rangle$.

Now, let us consider the case where the dimension of the image $\mathbf{t}_{V_1}(V_1^*)$ is two. Since the image is $\mathbb{P}^1$ in $\mathbb{P}(\mathbb{C}^2 \otimes \mathbb{C}^2)$, we have to investigate pencils of 2×2 matrices. By the discussion above, $\mathbf{t}_{V_1}(V_1^*)$ is exactly one of the N_1, N_2, N_3' and N_4' up to $GL(2) \times GL(2)$ action. Let us consider the case where $\mathbf{t}_{V_1}$ is N_3', i.e. $\mathbf{t}_{V_1}$ is spanned by the vectors $|00\rangle + |11\rangle$ and $|01\rangle$. If we write

$$\mathbf{t}_{V_1}(\langle 0|) = \alpha(|00\rangle + |11\rangle) + \beta|01\rangle,$$
$$\mathbf{t}_{V_1}(\langle 1|) = \gamma(|00\rangle + |11\rangle) + \delta|01\rangle,$$

for some $\alpha, \beta, \gamma, \delta \in \mathbb{C}$. Then $\mathbf{t}$ should be the vector

$$(\alpha|0\rangle + \gamma|1\rangle) \otimes (|00\rangle + |11\rangle) + (\beta|0\rangle + \delta|1\rangle) \otimes |01\rangle.$$

For generic $\alpha, \beta, \gamma, \delta \in \mathbb{C}$, $\mathbf{t}$ can be put into the following simpler form under the G-action:

$$|110\rangle + |101\rangle + |011\rangle$$

In the same way, we associate to each N_1, N_2 and N_4' the simplest form of

$\mathbf{t}$ as follows:

$$N1 : |110\rangle + |011\rangle, \quad N_2 : |101\rangle + |011\rangle, \quad N_4' : |000\rangle + |111\rangle.$$

Therefore, there are exactly 6 G-orbits given in the statement. □

Now we investigate geometric properties of the orbits. Since the projective space $\mathbb{P}^n$ is a $GL(n+1)$-homogeneous space, the orbit $O_1 = G \cdot |000\rangle$ is the closed orbit. Moreover, it is exactly the Segre variety $Seg(\mathbb{P}(V_1) \times \mathbb{P}(V_2) \times \mathbb{P}(V_3))$ and its dimension is 3. The orbit $O_2 = G \cdot (|101\rangle + |110\rangle) = G \cdot (|1\rangle \otimes (|01\rangle + |10\rangle))$ is obviously an element of

$$Y = Seg\left(\mathbb{P}(V_1) \times \sigma_2\left(Seg\left(\mathbb{P}(V_2) \times \mathbb{P}(V_3)\right)\right)\right).$$

Note that $\overline{(GL(2) \times GL(2)) \cdot (|01\rangle + |10\rangle)} = \sigma_2\left(Seg\left(\mathbb{P}^1 \times \mathbb{P}^1\right)\right) = \mathbb{P}^3$ by the discussion of the bipartite cases. Hence, the orbit closure $\overline{O_2}$ and Y are the same. In the same way, we can easily check that

$$\overline{O_3} = Seg\left(\mathbb{P}(V_2) \times \sigma_2\left(Seg\left(\mathbb{P}(V_1) \times \mathbb{P}(V_3)\right)\right)\right),$$
$$\overline{O_4} = Seg\left(\mathbb{P}(V_3) \times \sigma_2\left(Seg\left(\mathbb{P}(V_1) \times \mathbb{P}(V_2)\right)\right)\right).$$

Now let us consider the orbit $O_6 = G \cdot (|000\rangle + |111\rangle)$. By Example 2.7.7,

$$\overline{O_6} = \sigma(O_1) = \mathbb{P}(\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2).$$

Since this orbit has the expected dimension 7, the tangential variety $\tau(O_1)$ has the dimension 6 by Theorem 2.7.9. By Example 2.7.4, $\tau(O_1)$ contains the element $|110\rangle + |101\rangle + |011\rangle$, so does $G \cdot (|110\rangle + |101\rangle + |011\rangle)$. By Terracini's lemma, we can check that the dimension of the orbit $G \cdot (|110\rangle + |101\rangle + |011\rangle)$ is 6, so it is exactly the orbit $\overline{O_5}$ by the irreduciblility. Interestingly, the orbit $\overline{O_5}$ is exactly the dual of the variety O_1. It follows from the fact that the dual variety $O_1^\vee$ has dimension 6 by Theorem 2.8.4 and the G-invariant subvariety of dimension 6 is unique and it is exactly $\overline{O_5}$. Therefore, the generic elements in the whole space $\overline{O_6}$ and in $\overline{O_5}$ are distinguished by the hyperdeterminant given in Example 2.8.7. All the other orbits are distinguished by

the rank condition. For instance, a generic element $\mathbf{t}$ in the orbit $\overline{O_2}$ is separable when it is considered as an element in the bipartite quantum system consisting of V_1 and $V_2 \otimes V_3$, so $\mathbf{t}$ has rank one when we think of them as linear maps $V_1^* \longrightarrow V_2 \otimes V_3$. In this case, it is said that $\mathbf{t}$ has local rank one with respect to V_1. In the same way, we easily check that $\mathbf{t}$ has local rank two with respect to V_2 and V_3 respectively. Let $\mathbf{r}(\mathbf{t}) = (r_1, r_2, r_3)$ denotes the triple of local ranks of the tensor $\mathbf{t}$ with respect to V_1, V_2 and V_3. For instance, a generic element of $\overline{O_2}$ has local rank $(1, 2, 2)$. Similarly, generic elements of $\overline{O_3}$, $\overline{O_4}$ and $\overline{O_5}$ have local ranks $(2, 1, 2)$, $(2, 2, 1)$ and $(2, 2, 2)$ respectively. To summarize, all the orbits have the following stratification:

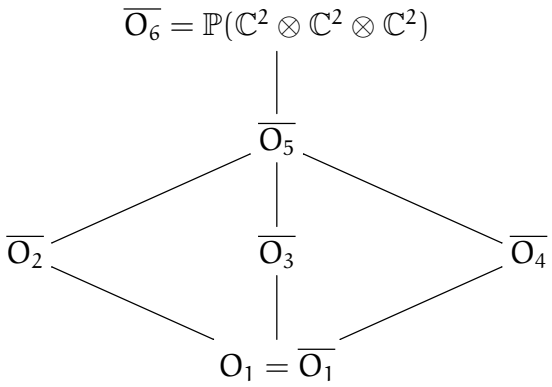

Figure 6.1: Orbit closures for the $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ case

6.3 Other cases

Under the action of SLOCC, there are finitely many orbits only when the following cases [Kac80]:

(i) $\mathbb{C}^m \otimes \mathbb{C}^n$

(ii) $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^n$

(iii) $\mathbb{C}^2 \otimes \mathbb{C}^3 \otimes \mathbb{C}^n$

for every $m, n \geq 2$. Moreover, their orbits are classified explicitly [HLT12, BL13]. For instance, we can obtain exactly 17 orbits for the $\mathbb{C}^2 \otimes \mathbb{C}^3 \otimes \mathbb{C}^3$ case using the same methods for the three qubit case. See [Lan12, Chapter 10] for more details. Therefore, it is the interesting cases that there are infinitely many orbits. For $n \geq 2$, The n qubit cases are such things. For these cases, even though there are attempts to find all the generators in the ring of invariant polynomials by taking advantage of the method of transvectants, which is the classical method to find invariants in the classical invariant theory [LT03, BLT03, LT06, ĐO09, HLT14], it is far from classifying the all orbits yet.

Bibliography

[ADR82] A. Aspect, J. Dalibard, and G. Roger. Experimental test of Bell's inequalities using time-varying analyzers. *Phys. Rev. Lett.*, 49(25):1804, 1982. 2

[Agr06] M. Agrawal. Determinant versus permanent. In *Proceedings oh the International Congress of Mathematicians: Madrid, August 22-30, 2006: invited lectures*, pages 985–998, 2006. 61

[AM69] M. F. Atiyah and I. G. Macdonald. *Introduction to Commutative Algebra*, volume 19. Addison-Wesley Reading, 1969. 12, 15

[BB84] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, volume 175, page 8. New York, 1984. 2

[BBC+93] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70(13):1895, 1993. 2

[Bel64] J. S. Bell. On the Einstein-Rosen-Podolsky paradox. *Physica*, 1:195, 1964. 2

[Ber75] D. N. Bernstein. The number of roots of a system of equations. *Functional Anal. Appl.*, 9(3):183–185, 1975. 55

[BL13] J. Buczyński and J. M. Landsberg. Ranks of tensors and a generalization of secant varieties. *Linear Algebra Appl.*, 438(2):668–689, 2013. 122, 126

[BLT03] E. Briand, J.-G. Luque, and J.-Y. Thibon. A complete set of covariants of the four qubit system. *J. Phys. A*, 36(38):9915, 2003. 126

[Boh35] N. Bohr. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 48(8):696–702, 1935. 1

[BW92] C. H. Bennett and S. J. Wiesner. Communication via one-and two-particle operators on Einstein-Podolsky-Rosen states. *Phys. Rev. Lett.*, 69(20):2881, 1992. 2

[CĐ13] L. Chen and D. Z. Đoković. Dimensions, lengths, and separability in finite-dimensional quantum systems. *J. Math. Phys.*, 54:022201, 2013. 107

[Cay45] A. Cayley. On the theory of linear transformations. *Cambridge Math. J*, 4(1845):1–16, 1845. 47

[Cho82] M.-D. Choi. Positive linear maps. *Proc. Sympos. Pure Math.*, 38:583–590, 1982. 65, 66, 67, 70

[CHSH69] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, 1969. 2

[CLO05] D. A. Cox, J. Little, and D. O'shea. *Using algebraic geometry,* 2nd ed. Springer, 2005. 53

[Deu85] D. Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, 400(1818):97–117, 1985. 2

[DLMV88] P. Dagum, M. Luby, M. Mihail, and U. Vazirani. Polytopes, permanents and graphs with large factors. In *Foundations of Computer Science, 1988., 29th Annual Symposium on*, pages 412–421. IEEE, 1988. 61

[DTT00] D. P. Divincenzo, B. M. Terhal, and A. V. Thapliyal. Optimal decompositions of barely separable states. *J. Modern Opt.*, 47(2-3):377–385, 2000. 107

[DVC00] W. Dür, G. Vidal, and J. I. Cirac. Three qubits can be entangled in two inequivalent ways. *Phys. Rev. A*, 62(6):062314, 2000. 9

[Eke91] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67(6):661–663, 1991. 2

[EPR35] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47(10):777, 1935. 1

[FC72] S. J. Freedman and J. F. Clauser. Experimental test of local hidden-variable theories. *Phys. Rev. Lett.*, 28(14):938, 1972. 2

[FH79] W. Fulton and J. Hansen. A connectedness theorem for projective varieties, with applications to intersections and singularities of mappings. *Ann. of Math.*, 110(1):159–166, 1979. 47

[FOV99] H. Flenner, L. O'Carroll, and W. Vogel. *Joins and Intersections*. Springer, 1999. 45

[Ful93] W. Fulton. *Introduction to toric varieties*, volume 131. Princeton University Press, 1993. 54

[Gan60] F. R. Gantmacher. *The theory of matrices*, volume 2. Taylor & Francis, 1960. 121

[GH11] P. Griffiths and J. Harris. *Principles of algebraic geometry*, volume 52. John Wiley & Sons, 2011. 29, 36, 49

[Gha10] S. Gharibian. Strong NP-hardness of the quantum separability problem. *Quantum Inf. Comput.*, 10(3):343–360, 2010. 7, 62

[GK87] D. Y. Grigoriev and M. Karpinski. The matching problem for bipartite graphs with polynomially bounded permanents is in NC. In *Foundations of Computer Science, 1987., 28th Annual Symposium on*, pages 166–172. IEEE, 1987. 61

[GKZ92] I. M. Gelfand, M. M. Kapranov, and A. V. Zelevinsky. Hyperdeterminants. *Adv. in Math.*, 96(2):226–263, 1992. 47

[GKZ08] I. M. Gelfand, M. M. Kapranov, and A. V. Zelevinsky. *Discriminants, Resultants, and Multidimensional Determinants*. Birkhäuser Boston, 2008. 50, 51, 60

[Gur03] L. Gurvits. Classical deterministic complexity of Edmonds' Problem and quantum entanglement. In *Proceedings of the Thirty-Fifth Annual ACM Symposium on Theory of Computing*, STOC '03, pages 10–19, New York, NY, USA, 2003. ACM. 7, 62

[Har77] R. Hartshorne. *Algebraic Geometry*. Number 52. Springer, 1977. 20, 23, 33, 78, 81

[Har92] J. Harris. *Algebraic Geometry: A First Course*, volume 133. Springer, 1992. 25, 26, 35

[Hat02] A. Hatcher. *Algebraic Topology*. Cambridge University Press, 2002. 29, 41

[HHH96] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of mixed states: necessary and sufficient conditions. *Phys. Lett. A*, 223(1):1–8, 1996. 66

[Hir76] M. W. Hirsch. Differential topology. *Graduate Texts in Mathematics*, 1976. 79, 81

[HK04] K.-C. Ha and S.-H. Kye. Construction of entangled states with positive partial transposes based on indecomposable positive linear maps. *Phys. Lett. A*, 325(5):315–323, 2004. 67

[HK13] K.-C. Ha and S.-H. Kye. Geometry for separable states and construction of entangled states with positive partial transpose. *Phys. Rev. A*, 88:024302, 2013. 10, 107, 110

[HK14] K.-C. Ha and S.-H. Kye. Separable States with Unique Decompositions. *Comm. Math. Phys.*, 328(1):131–153, 2014. 10, 107, 108

[HKP03] K.-C. Ha, S.-H. Kye, and Y. S. Park. Entangled states with positive partial transposes arising from indecomposable positive linear maps. *Phys. Lett. A*, 313(3):163–174, 2003. 67

[HLT12] F. Holweck, J.-G. Luque, and J.-Y. Thibon. Geometric descriptions of entangled states by auxiliary varieties. *J. Math. Phys.*, 53(10):102203, 2012. 122, 126

[HLT14] F. Holweck, J.-G. Luque, and J.-Y. Thibon. Entanglement of four qubit systems: A geometric atlas with polynomial compass I (the finite world). *J. Math. Phys.*, 55(1):012202, 2014. 126

[HLVC00] P. Horodecki, M. Lewenstein, G. Vidal, and J. I. Cirac. Operational criterion and constructive checks for the separability of low-rank density matrices. *Phys. Rev. A*, 62(3):032310, 2000. 73

[Hor97] P. Horodecki. Separability criterion and inseparable mixed states with positive partial transposition. *Phys. Lett. A*, 232(5):333–339, 1997. 66, 68, 107, 113

[HSYY08] P. Huggins, B. Sturmfels, J. Yu, and D. Yuster. The hyperdeterminant and triangulations of the 4-cube. *Math. Comp.*, 77(263):1653–1679, 2008. 51

[Hul03] K. Hulek. *Elementary Algebraic Geometry*. Number 20. American Mathematical Soc., 2003. 13, 16

[Kac80] V. G. Kac. Some remarks on nilpotent orbits. *J. Algebra*, 64(1):190–213, 1980. 125

[KCKL00] B. Kraus, J. I. Cirac, S. Karnas, and M. Lewenstein. Separability in $2 \times N$ composite quantum systems. *Phys. Rev. A*, 61:062302, 2000. 73

[KKL11] Y.-H. Kiem, S.-H. Kye, and J. Lee. Existence of product vectors and their partial conjugates in a pair of spaces. *J. Math. Phys.*, 52(12):122201, 2011. 9, 73, 76, 84, 87

[KS83] A. R. Kräuter and N. Seifter. On some questions concerning permanents of $(1, -1)$-matrices. *Israel J. Math.*, 45(1):53–62, 1983. 89

[Kye12] S.-H. Kye. Facial structures for various notions of positivity and applications to the theory of entanglement. *Rev. Math. Phys.*, 25:1330002, 2012. 67, 70

[Kye13] S.-H. Kye. Faces for two qubit separable states and the convex hulls of trigonometric moment curves. *arXiv:1302.2226*, 2013. 10, 107

[Lan12] J. M. Landsberg. *Tensors: Geometry and applications*, volume 128. American Mathematical Soc., 2012. 126

[Laz04] R. K. Lazarsfeld. *Positivity in algebraic geometry I: Classical setting: line bundles and linear series*, volume 48. Springer, 2004. 47

[LP98] N. Linden and S. Popescu. On multi-particle entanglement. *Fortschritte der Physik*, 46:567–578, 1998. 9

[LT03] J.-G. Luque and J.-Y. Thibon. Polynomial invariants of four qubits. *Phys. Rev. A*, 67(4):042303, 2003. 126

[LT06] J.-G. Luque and J.-Y. Thibon. Algebraic invariants of five qubits. *J. Phys. A*, 39(2):371, 2006. 126

[LW96] T. Y. Li and X. Wang. The BKK Root Count in $\mathbb{C}^n$. *Math. Comp.*, 65(216):pp. 1477–1484, 1996. 55

[Mat89] H. Matsumura. *Commutative Ring Theory*, volume 8. Cambridge university press, 1989. 14

[McC04] W. McCuaig. Pólya's permanent problem. *Electron. J. Combin*, 11(1):R79, 2004. 61

[Min84] H. Minc. *Permanents*, volume 6. Cambridge University Press, 1984. 60

[Mui03] T. Muir. *A Treatise on the Theory of Determinants*. Courier Dover Publications, 2003. 47

[ĐO09] D. Z. Đoković and A. Osterloh. On polynomial invariants of several qubits. *J. Math. Phys.*, 50(3):033509, 2009. 126

[Osa91] H. Osaka. Indecomposable positive maps in low dimensional matrix algebras. *Linear Algebra Appl.*, 153:73–83, 1991. 67

[Osa93] H. Osaka. A series of absolutely indecomposable positive maps in matrix algebras. *Linear Algebra Appl.*, 186:45–53, 1993. 67

[Ott13] G. Ottaviani. Introduction to the hyperdeterminant and to the rank of multidimensional matrices. In *Commutative Algebra*, pages 609–638. Springer, 2013. 52

[Per96] A. Peres. Separability Criterion for Density Matrices. *Phys. Rev. Lett.*, 77:1413–1415, 1996. 65

[RW09] M. B. Ruskai and E. M. Werner. Bipartite states of low rank are almost surely entangled. *J. Phys. A*, 42(9):095303, 2009. 73

[Sho95] P. W. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, 52(4):R2493, 1995. 2

[SS83] R. Simion and F. W. Schmidt. On $(+\mathbf{1}, -\mathbf{1})$-matrices with vanishing permanent. *Discrete Math.*, 46(1):107–108, 1983. 89, 93

[TV09] T. Tao and V. Vu. On the permanent of random bernoulli matrices. *Adv. in Math.*, 220(3):657–669, 2009. 96

[VN55] J. Von Neumann. *Mathematical foundations of quantum mechanics*. Number 2. Princeton university press, 1955. 1

[VW02] K. G. Vollbrecht and M. M. Wolf. Conditional entropies and their relation to entanglement criteria. *J. Math. Phys.*, 43(9):4299–4306, 2002. 66

[Wan74] E. T.-H. Wang. On permanents of (1, -1)-matrices. *Israel J. Math.*, 18(4):353–361, 1974. 89

[Wan05] I. M. Wanless. Permanents of matrices of signed ones. *Linear and Multilinear Algebra*, 53(6):427–433, 2005. 89

[Wer89] R. F. Werner. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Phys. Rev. A*, 40:4277–4281, Oct 1989. 6

[Wor76] S. L. Woronowicz. Positive maps of low dimensional matrix algebras. *Rep. Math. Phys.*, 10(2):165–183, 1976. 66, 67

[WS08] J. Walgate and A. J. Scott. Generic local distinguishability and completely entangled subspaces. *J. Phys. A*, 41(37):375305, 2008. 73, 101

[Zak05] F. L. Zak. *Tangents and Secants of Algebraic Varieties*, volume 127. American Mathematical Soc., 2005. 47

국문초록

이 논문에서 우리는 대수기하학의 다양한 방법들을 이용하여 양자 상태의 분리 가능성 문제를 연구한다.

양자 상태의 분리가능성 문제를 연구하기위해 양자 분리 가능성에 관한 치역 판별법으로부터 시작하는데, 이 판별법에 따르면 주어진 유한차원 복합 양자계의 두 부분공간 D와 E에 대하여 $|\psi_1\rangle \otimes |\psi_2\rangle \in \mathsf{D}$이고 $|\overline{\psi_1}\rangle \otimes |\psi_2\rangle \in \mathsf{E}$인 곱벡터 $|\psi_1\rangle \otimes |\psi_2\rangle$을 조사하는 것이 자연스럽다.

우리는 이 문제를 다음과 같은 두 가지 문제로 분리하여 생각한다. (1) 어떤 조건에 대하여 $|\psi_1\rangle \otimes |\psi_2\rangle \in \mathsf{D}$ and $|\overline{\psi_1}\rangle \otimes |\psi_2\rangle \in \mathsf{E}$를 만족하는 $\mathcal{H}_A \otimes \mathcal{H}_B$의 영이 아닌 곱벡터 $|\psi_1\rangle \otimes |\psi_2\rangle$가 존재하는가? (2) 만약 존재한다면, 그 조건을 만족하는 영이 아닌 곱벡터가 얼마나 많이 존재하는가?

우리는 문제 (1)을 조사하고 이를 다입자 양자계의 경우로 확장한다. 또한 문제 (2)에 대하여 $|\psi_1\rangle \otimes |\psi_2\rangle \in \mathsf{D}$ and $|\overline{\psi_1}\rangle \otimes |\psi_2\rangle \in \mathsf{E}$ 조건을 만족하는 곱벡터 $|\psi_1\rangle \otimes |\psi_2\rangle$의 갯수의 상한값을 제시하는데, 이는 큐빗-큐닛인 경우에 정확한 상한값일 것으로 예상된다.

주요어휘: 양자얽힘, 분리가능 상태, 얽힌 상태, 곱벡터, 치역판별법, 대수기하학
학번: 2006-20294