Univerzita Palackého v Olomouci
Přírodovědecká fakulta
Katedra optiky

BAKALÁŘSKÁ PRÁCE

Minimal criterion for continuous-variable genuine multipartite quantum steering

Vypracoval:	**Tadeáš Volný**
Studijní obor:	Obecná fyzika a matematická fyzika
Forma studia:	Prezenční
Vedoucí diplomové práce:	doc. Mgr. Ladislav Mišta, Ph.D.
Rok odevzdání práce:	2023

Prohlášení

Prohlašuji, že jsem předloženou bakalářskou práci vypracoval samostatně pod vedením Ladislava Mišty a že jsem použil zdrojů, které cituji a uvádím v seznamu použitých pramenů.

Tadeáš Volný

Bibliografická identifikace

Jméno a příjmení autora	Tadeáš Volný
Název práce	Minimal criterion for continuous-variable genuine multipartite quantum steering
Typ práce	Bakalářská
Pracoviště	Katedra optiky
Vedoucí práce	doc. Mgr. Ladislav Mišta, Ph.D.
Rok obhajoby práce	2023
Abstrakt	Kvantový steering je druh kvantových korelací, který je silnější než provázanost, ale slabší než Bellova nelokalita. Představíme-li si dvě strany sdílející bipartitní kvantový stav, pak řekneme, že tento stav je steerovatelný, jestliže pro všechna možná měření na jedné části stavu nelze množinu indukovaných podmíněných stavů druhé části vysvětlit prostřednictvím tzv. modelu lokálních skrytých stavů. Steering se stal významným prostředkem pro jednostrannou, na zařízení nezávislou distribuci kvantového klíče nebo diskriminaci podkanálů. V této práci se budeme zabývat multipartitním kvantovým steeringem pro systémy s nekonečně rozměrnými Hilbertovými stavovými prostory. Konkrétně se zaměříme na odvození nového kritéria pro nejsilnější formu steeringu, tzv. skutečný multipartitní steering. Na rozdíl od stávajících kritérií, která obvykle obsahují kombinace kvadratur všech uvažovaných módů, bude cílem této práce nalézt minimální kritérium zahrnující nejmenší počet nejvýše dvoumódových kombinací operátorů kvadratur. Praktická použitelnost získaného kritéria bude následně demonstrována na detekci skutečného multipartitního steeringu několika třímodových Gaussovských stavů.
Klíčová slova	kvantový steering, skutečně multipartitní steering, spojité proměnné
Počet stran	44
Počet příloh	0
Jazyk	anglický

Bibliographical identification

Autor's first name and surname	Tadeáš Volný
Title	Minimal criterion for continuous-variable genuine multipartite quantum steering
Type of thesis	Bachelor
Department	Department of Optics
Supervisor	doc. Mgr. Ladislav Mišta, Ph.D.
The year of presentation	2023
Abstract	Quantum steering is a class of quantum correlations that is stronger than entanglement but weaker than Bell's nonlocality. If we imagine two parties sharing a bipartite quantum state, then we say that this state is steerable if, for all possible measurements on one part of the state, the set of induced conditional states of the other part cannot be explained by the so-called local-hidden-state model. Steering has become an important resource for one-sided device-independent quantum key distribution or subchannel discrimination. In this thesis, we will discuss multipartite quantum steering for systems with infinite-dimensional Hilbert state spaces. Specifically, we will derive a new criterion for the strongest form of steering, called genuine multipartite steering. In contrast to existing criteria, which usually contain combinations of quadratures of all considered modes, the goal of this work will be to find a minimal criterion involving a minimum number of at most two-mode combinations of quadrature operators. Practical utility of the obtained criterion will be then demonstrated on its ability to detect genuine multipartite steering of several three-mode Gaussian states.
Keywords	quantum steering, genuine multipartite steering, continuous variables
Number of pages	44
Number of appendices	0
Language	english

Contents

Chapter 1

Introduction

For centuries, scientists have explored the mysteries of our universe. Many of them are still hidden from us, but of the mysteries we have already discovered, quantum mechanics is perhaps the most fascinating. The quantum world, that is, the world of subatomic particles, operates on principles completely different from those to which we are accustomed. One of the most interesting phenomena in the quantum world is quantum correlations. Especially recently, these have become a valuable resource for quantum metrology, cryptography, and secure communication systems.

In this thesis, we will discuss the younger brother of entanglement – quantum steering. We will derive a new criterion for genuine tripartite steering and afterward use it to detect genuine tripartite steerable states. Quantum correlations are non-intuitive phenomena and there are no analogies in classical physics by which we can explain them. However, if one wanted to explain steering in a somewhat classical way, one might say the following. Imagine you are watching someone driving a car, an ordinary unmodified car. Now imagine that, no matter how far away you are, you are capable of remotely controlling, or let's say steering, this car without touching the steering wheel. Of course, this sounds absurd, because macroscopic objects cannot behave this way, but subatomic objects can, and this is precisely how steering works. Suppose now that two parties share an entangled state. In this situation, one party can "steer" the quantum state of the other party into a different state by making suitable measurements on its part of the entangled state.

Before we begin to explore steering from a physical point of view, it might be useful to put the concept into a historical context. The most convenient approach would be to start with a well-known article from 1935 by Albert Einstein, Boris Podolsky, and Nathan Rosen [1]. The EPR article[1] has opened the door for the study of quantum correlations. EPR present a thought experiment that uses entanglement to show that the quantum-mechanical description of the world is not complete. Entanglement is a phenomenon in which two particles are correlated in such a way that a measurement of one particle will change the state of the other particle, no matter how far apart they are. Why is this mentioned in this thesis and how is it connected to steering? Consider two entangled particles, if we measure a property of one particle, then we immediately know the corresponding property of the other particle regardless of the

[1]EPR is an abbreviation formed from the first letters of the authors' last names – Einstein, Podolsky, Rosen. Today, this article is usually referred to as an "EPR article". However, the original title is "*Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?*".

distance between them. Steering allows us by measuring the properties of one party to change, i.e. to steer, the quantum state of the other party to a different state. The resemblance is self-evident as both of these phenomena enable us to remotely control quantum states. And given that only pure quantum states for which entanglement, steering, and Bell nonlocality coincide were considered at the time, it can be argued that the EPR paper concealed a greater treasure than might have been expected back then. Erwin Schrödinger responded to the EPR paper in October 1935[2] [2]. The following is a quote directly from this article: "*It is rather discomforting that the theory should allow a system to be steered or piloted into one or the other type of state at the experimenter's mercy in spite of his having no access to it.*" Although Schrödinger responds with this quote to the EPR article that discusses entanglement, one cannot help but notice that this sentence can also be applied to steering, and that, moreover, the word "steered" is directly used in the text. The term "steering" in fact comes from this quote.

As already mentioned, for a very long time only pure quantum states were considered, for which entanglement, steering and nonlocality merge. This has hindered the individual correlations from being examined in detail. This didn't change until the 1980s, most notably in an article by R. Werner in 1989 [3]. Werner's paper studies the possibility of constructing a hidden-variable model for entangled mixed quantum states involving EPR correlations. This means that there exists a way to explain quantum correlations without the need to take nonlocality into account. We didn't have a proper definition of quantum steering until 2007 and it was presented by Wiseman, Jones, and Doherty in their two articles [4, 5]. These two papers analyze the three named correlations, provide operational and mathematical definitions and establish a hierarchy between them.

Surely it is worthwhile to mention at least a few experiments in which steering has been demonstrated. It is noteworthy to mention that steering can be both one-way and two-way. If we imagine two parties, say, Alice and Bob, then the systems can be correlated in such a way that only Alice can steer Bob's system, but not vice versa. This is one-way steering. But their systems can be correlated in such a manner that it works both ways – two-way steering. The first demonstration of this effect was accomplished by Ou et al. in 1992 [6], later in 2008 two-way steering was demonstrated [7]. Let us now examine a few experiments in more detail.

In a 2012 experiment [8] the team of Händchen et al. proposed and experimentally demonstrated one-way steering with two-mode squeezed states. They generated a pair of entangled photons which were measured subsequently using a combination of half-waveplates and polarizing beam splitters with the addition of a homodyne detection technique that measured quadrature amplitudes to show that only Alice can steer Bob, but not vice versa.

Furthermore, a 2012 article by Wittmann et al. [9], in which a loophole-free EPR experiment via quantum steering was achieved. They presented the first loophole-free demonstration of EPR steering using polarization-entangled photons shared between two distant laboratories. Their experiment simultaneously closed all loopholes: the locality loophole and the freedom-of-choice loophole by having a large separation of the parties and using fast quantum random number generators, and the fair-sampling loophole by using high-efficiency detectors.

Last, to be mentioned here is a 2020 experiment performed by Wollmann et al. [10]. Again, in this experiment, a pair of entangled photons was generated. The

[2]EPR article was published on May 15, 1935.

photons were then separated and sent to two distant laboratories. The measurement was conducted using a combination of waveplates, polarizing beam splitters, and single-photon detectors. In conclusion, they have experimentally demonstrated steering using generalized entropic criteria.

The experiments listed here are certainly not the only ones of their kind, but it is enough to show that steering is an experimentally observable effect.

Besides the experiments, we should also mention the applications of this phenomenon. One of the areas where steering is exploited is *one-sided device-independent quantum key distribution* (1SDI-QKD) [12]. First of all, let us take a look at what quantum key distribution (QKD) is. QKD is a secure communication method that enables two parties, say, Alice and Bob, to create a random secret key at a distance that can then be used to encrypt and decrypt messages. The security of such communication is given by the laws of quantum mechanics[3]. Alice and Bob share two channels: a quantum one, which allows them to share quantum signals, and a classical one, through which they can send classical messages. Their job is to ensure security against an eavesdropper, usually called Eve, which can connect to the quantum channel and listen to their exchanges on the classical channel. In standard QKD (S-QKD or simply QKD), safety is usually established under the condition that Alice and Bob can trust the functioning of their preparation and measurement apparatuses. Another kind, device-independent QKD (DI-QKD), can only establish security based on observation of violation of Bell inequalities, as we do not trust the measurement apparatuses. Nevertheless, DI-QKD places very demanding requirements on practical demonstrations [12].

Between S-QKD and DI-QKD lies 1SDI-QKD. The article [12] describes how 1SDI-QKD could be used in real life: Imagine that a bank wants to set up secret keys with its clients; the bank would invest a lot of money in setting up one trusted measurement device, but the clients at the other end of the channel would surely have cheap detection terminals. They later show that the detector efficiency required to implement 1SDI-QKD is much lower than that of DI-QKD, making it achievable with existing devices. Each of the three types of QKD corresponds to a different criterion for quantum correlations. The S-QKD requires that the observed correlations violate a separability criterion (i.e., entanglement is demonstrated), the DI-QKD requires a violation of Bell's inequality, and the 1SDI-QKD requires that the correlations violate a steering inequality.

Steering can also be used in *subchannel discrimination*. This is a protocol for decomposition of a channel into subchannels and it can also be interpreted as identification of which branch of an evolution a quantum system undergoes. Entanglement between a probe and an ancilla can help in discriminating different channels. We know that all steerable states are entangled, but not all entangled states are steerable. And if the measurements are limited to local operations and forward communication (one-way LOCC), then only the steerable states remain useful [13].

To be able to exploit steering, we first need to find states that exhibit it; this may be done via steering criteria. Moreover, we do not wish to only demonstrate steering between two parties, i.e. bipartite steering, but multipartite, where, for example, Alice and Bob are joined by Charlie and then perhaps others. Detection of bipartite steering let alone multipartite steering is very challenging and deriving such a criterion is no

[3]For details on how this security is accomplished, see article [11].

simple task. One of the first criteria can be found in [14]. Many criteria have been derived since then, but the vast majority refer to bipartite steering. This implies that we require more criteria for multipartite steering. And preferably, for these criteria to require minimal knowledge about the measured state – to be the so-called minimal criteria. An example of one of the latest such criteria is given in [16]. This criterion is designed to detect genuine multipartite steering (GMS) for which we provide here a brief definition: A state contains genuine multipartite steerable correlations if they cannot be produced by mixing states with only bipartite steering relative to different bipartite splits [15]. Regarding the criteria for GMS, one can say that they represent a gap in this field of research. Our criterion might help to fill this gap. We derived a criterion that not only does not require complete information about the measured state, but moreover is not designed for a specific state, but rather designed to search for GMS states.

1.1 Introduction to quantum mechanics

This thesis deals with a subject that is grounded in quantum mechanics, therefore we start with a brief introduction to quantum theory. Rigorous definitions of the mathematical terms used in this introduction can be found in the Mathematical supplement. When writing these fundamental principles of quantum theory, we have used the books [17, 18].

1.1.1 Postulates of quantum mechanics

We will first state several postulates. Their structure does not correspond to the standard layout, nevertheless, we include everything necessary to grasp the essentials of this work.

Postulate I

(a) To each quantum system corresponds a separable complex Hilbert space $\mathscr{H}$, which we call the state space of the system.

(b) To each state of the considered system corresponds a ray $\Psi = \{\lambda \left|\psi\right\rangle , \lambda \in \mathbb{C}\}$[4], i.e. a one-dimensional subspace in $\mathscr{H}$.

Postulate II

a) To each measurable physical quantity, i.e. an observable, of a given system corresponds a Hermitian operator $\hat{A}$ on $\mathscr{H}$.

b) The possible results of the measurement of $\hat{A}$ are the eigenvalues of this operator. The probability of measuring the eigenvalue a is equal to

$$p_a = \left\langle\psi\right| \hat{P}_a \left|\psi\right\rangle , \tag{1.1}$$

where $\hat{P}_a$ is a projection operator which projects onto the subspace corresponding to the value of a.

[4]Usually the difference between the ray Ψ and the vector $|\psi\rangle$ is neglected.

c) The expectation value of the results of the measurement is

$$\langle \hat{A} \rangle = \langle \psi | \, \hat{A} \, | \psi \rangle \, . \tag{1.2}$$

The eigenvalues of the Hermitian operator are real numbers and can therefore describe measurement results that are also real. The eigenvectors of a Hermitian operator corresponding to different eigenvalues are orthogonal and form a basis in $\mathscr{H}$. With each Hermitian operator $\hat{A}$ of each observable there is associated a set of eigenvalues $\{a\} = \sigma(\hat{A})$ (the so-called spectrum of the operator $\hat{A}$) and a set of projection operators $\{\hat{P}_a : \, |a\rangle \langle a|\}$, $a \in \sigma(\hat{A})$, where these projection operators project onto orthogonal subspaces in $\mathscr{H}$ and decompose the unit (completeness relation)

$$\sum_a \hat{P}_a = \sum_a |a\rangle \langle a| = \mathbb{1}. \tag{1.3}$$

Each Hermitian operator is associated with a measurement described by a set of projection operators.

States that are described by a ray (a normalized vector $|\psi\rangle$) are called *pure states*. Pure states contain the maximum available information about the state of the considered system. Not all states are pure, i.e. they cannot be described by a ray. Take a look at the following example (see Fig. 1.1).

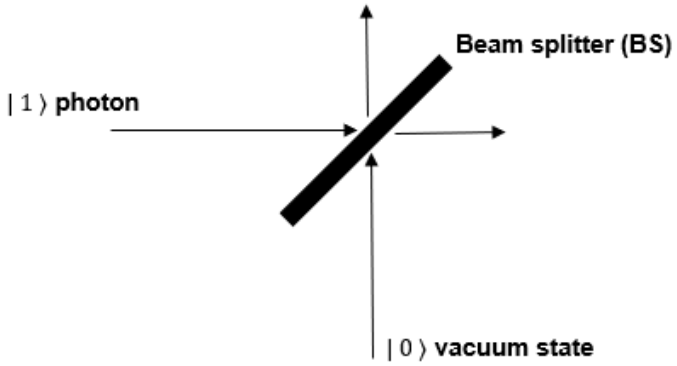

Figure 1.1: Scheme of a single-photon state.

A beam splitter (BS) is characterized by transmittance T and reflectance R, where $T^2 + R^2 = 1$. This state can be described as $T^2 \, |1\rangle \langle 1| + R^2 \, |0\rangle \langle 0|$, but it is no longer a state vector, i.e. this expression cannot be written as a projector $|\psi\rangle \langle \psi|$. We can describe this state by the so-called density matrix

$$\begin{pmatrix} T^2 & 0 \\ 0 & R^2 \end{pmatrix} \neq |\psi\rangle \langle \psi| \, . \tag{1.4}$$

Density matrix is a Hermitian positive semidefinite matrix with a trace equal to one.

Postulate III

a) To each state corresponds some density matrix ρ on the state space $\mathscr{H}$, which has the following properties

$$\rho = \rho^\dagger, \, \rho \geq 0, \, \mathrm{Tr}[\rho] = 1. \tag{1.5}$$

b) The probability of measuring the value of the observable $\hat{A}$ on the system in the state ρ is given by

$$p_a = \mathrm{Tr}[\rho \hat{P}_a]. \tag{1.6}$$

c) The expectation value of the results of the measurement is

$$\langle \hat{A} \rangle_\rho = \mathrm{Tr}[\rho \hat{A}] = \sum_i p_i \langle \psi_i | \hat{A} | \psi_i \rangle = \sum_i p_i \langle \hat{A} \rangle_{\psi_i}. \tag{1.7}$$

In general, the density matrix is of the form

$$\rho = \sum_i p_i |\psi_i\rangle \langle \psi_i|, \, 0 \leq p_i \leq 1, \, \sum_i p_i = 1. \tag{1.8}$$

Postulate IV

If x_i and p_i are Cartesian canonically conjugate variables, then their operators satisfy commutation relations

$$[\hat{x}_i, \hat{p}_j] = i\hbar \delta_{ij}, \, [\hat{x}_i, \hat{x}_j] = [\hat{p}_i, \hat{p}_j] = 0, \, i = 1,2,...,n. \tag{1.9}$$

In the following, we will use operators without the hats ($\hat{A} \to A$).

1.1.2 Uncertainty relations

Let us introduce operators

$$\Delta A = A - \langle A \rangle, \, \Delta B = B - \langle B \rangle.^5 \tag{1.10}$$

We further introduce the variance

$$\langle (\Delta A)^2 \rangle = \langle (A - \langle A \rangle)^2 \rangle = \langle A^2 \rangle - \langle A \rangle^2. \tag{1.11}$$

Consider two non-commutative Hermitian operators A and B with commutator $[A,B] = iC$, where C is again a Hermitian operator. Take now the product of the variances of the operators A, B and we can derive that[6]

$$\langle (\Delta A)^2 \rangle \langle (\Delta B)^2 \rangle \geq \frac{1}{4} |\langle C \rangle|^2. \tag{1.12}$$

If we use the commutation relations for x and p (see Eq. (1.9)), we get the Heisenberg uncertainty relation

$$\langle (\Delta x)^2 \rangle \langle (\Delta p)^2 \rangle \geq \frac{\hbar^2}{4}. \tag{1.13}$$

[5] It is simple to prove that $\langle \Delta A \rangle = \langle A \rangle - \langle \langle A \rangle \rangle = \langle A \rangle - \langle A \rangle = 0$.

[6] See Appendix 1 for the derivation.

1.1.3 Composite systems

The state space of a composite system consisting of N subsystems is the tensor product of the subsystem state spaces, $\mathscr{H} = \mathscr{H}_1 \otimes \mathscr{H}_2 \otimes ... \otimes \mathscr{H}_N = \otimes_{i=1}^{N} \mathscr{H}_i$,[7] supposing that the subsystems are mutually distinct. We will discuss here an example of composite systems of two quantum bits (qubits). Consider two qubits with state space $\mathscr{H} = \mathscr{H}_A \otimes \mathscr{H}_B = \mathbb{C}_2 \otimes \mathbb{C}_2$. From the bases $\{|0\rangle_A, |1\rangle_A\}$ and $\{|0\rangle_B, |1\rangle_B\}$ on in the spaces $\mathscr{H}_A$ and $\mathscr{H}_B$ can be formed a product basis $\{|i\rangle_A, |j\rangle_B\}_{i,\, j\in\{0,\, 1\}}$.

Entangled states of two subsystems are states which are not of the previous form, i.e. they cannot be written as $|\varphi\rangle_A |\psi\rangle_B$, where $|\varphi\rangle_A \in \mathscr{H}_A$ and $|\psi\rangle_B \in \mathscr{H}_B$, therefore, they are not product states. States that can be written in this way are called *separable*. Let us now take a short detour to the entanglement of mixed states in order to introduce several terms. Local operations and classical communication (LOCC) play an important role in the theory of entanglement. A local operation (LO) is any operation allowed by quantum mechanics performed locally on one of the subsystems. Classical communication (CC) is the communication of classical information that can be arbitrarily perfectly copied and read without corruption and which can be perfectly discriminated. We say that a quantum state is entangled if it cannot be prepared by LOCC operations. The states that can be prepared by LOCC operations are called separable and are of the form [3]

$$\rho_{AB} = \sum_i \lambda_i \rho_A^{(i)} \otimes \rho_B^{(i)},$$

where $\rho_A^{(i)}$, $\rho_B^{(i)}$ are density matrices of subsystems A and B and λ_i are probabilities.

1.1.4 Continuous-variable systems

Consider N-mode[8] quantum system, which posseses a state space $\otimes_{i=1}^{N} \mathscr{H}_i$, where $\dim\mathscr{H} = \infty$. Essential physical quantities, used to describe modes, are the operators x and p [9], which are called *amplitude* and *phase quadrature operators*. These two quadrature operators satisfy the canonical commutation relation $[x, p] = \mathbb{1}$ resembling the commutation relation for operators of position and momentum (1.9). Both x and p have a continuous spectrum, therefore we can call them *contiuous variables* and we can call the respective systems *continuous-variable* (CV) systems. We now introduce a $2N \times 1$ vector of quadrature operators $\mathbf{r} = (x_1, ..., x_N, p_1, ..., p_N)^T$. The commutation relations for this vector can be compactly expressed as

$$[\mathbf{r}_j, \mathbf{r}_k] = i(\Omega_N)_{jk}, \tag{1.14}$$

where Ω_N is the so-called *symplectic matrix* defined as

$$\Omega_N = \oplus_{i=1}^{N} J = \oplus_{i=1}^{N} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{1.15}$$

[7] Let $\{|\psi_i\rangle\}_{i=1}^{n}$ and $\{|\varphi_j\rangle\}_{j=1}^{m}$ be the basis of Hilbert spaces $\mathscr{H}_1$, $\mathscr{H}_2$ respectively, where n, m are dimensions of the spaces. Then basis of $\mathscr{H}_1 \otimes \mathscr{H}_2$ will be $\{|\psi_i\rangle \otimes |\varphi_j\rangle\}_{i,j=1}^{n,m}$.

[8] We can think of a mode as a distribution of the electromagnetic field that is supported by a resonator. It can be called a mode of the resonator, which is described by some mode function that is a solution of Maxwell's equations in the resonator and thus depends on the shape of the resonator mirrors. It has its own frequency, wave vector, and polarization and does not have to be only in the resonator but can also be in free space. Simply put, it is any distribution of the field into the basis of some functions.

[9] For simplicity, from now on we will write operators without hats.

A special set of states corresponding to CV systems are *Gaussian states*.

1.1.5 Gaussian states

We are still considering the N-mode quantum system. For a single mode, we introduce the *phase space*, which is the space of eigenvalues of the operators $\hat{x}$ and $\hat{p}$. Since the eigenvalues of these operators can be any real number, this phase space is equivalent to the plane $\mathbb{R}^2$ (see Fig.1.2).

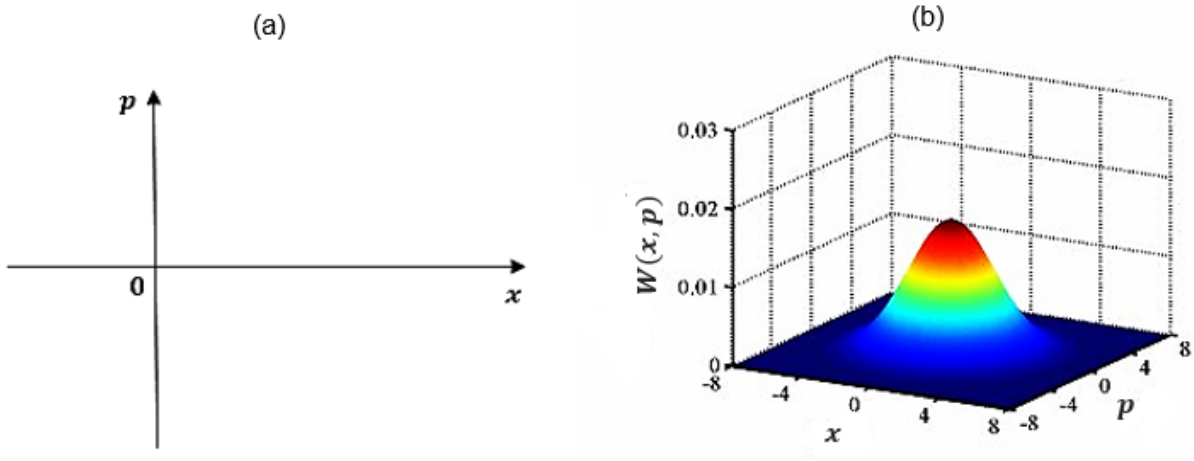

Figure 1.2: (a) Phase space of one mode. (b) The depicted Thermal state is a Gaussian state. Figure from [19] (the notation of the axes in the figure has been simplified compared to the original figure).

Any state ρ in phase space may be represented by a *Wigner function* [20]. We will now introduce everything for one mode and then generalize it to N-modes. We introduce the Weyl operator[10]

$$W(\xi) = e^{-i\boldsymbol{\xi}^T \mathbf{r}}, \tag{1.16}$$

where $\boldsymbol{\xi} = (\xi_x, \xi_p)^T$, $\xi_x, \xi_p \in \mathbb{R}$ and $\mathbf{r} = (x, p)^T$. Let us define the so-called characteristic function

$$C(\boldsymbol{\xi}) = \langle W(\boldsymbol{\xi}) \rangle = \mathrm{Tr}[\rho W(\boldsymbol{\xi})]. \tag{1.17}$$

We will perform a Fourier transform of the characteristic function

$$[\mathcal{F}C(\boldsymbol{\xi})](\mathbf{r}) = \frac{1}{2\pi} \int_{-\infty}^{\infty} e^{ix'p} \left\langle x - \frac{x'}{2} \right| \rho \left| x + \frac{x'}{2} \right\rangle dx' = W(\mathbf{r}) \tag{1.18}$$

resulting in the Wigner function $W(\mathbf{r})$. This can be generalized to the N-mode case:

$$W(\boldsymbol{\xi}) = e^{-i\boldsymbol{\xi}^T \mathbf{r}} = \Pi_{i=1}^{N} W_i(\boldsymbol{\xi}_\mathbf{i}), \tag{1.19}$$

where $W_i(\boldsymbol{\xi}_\mathbf{i}) = e^{-i\xi_i r_i}$, $\boldsymbol{\xi}_\mathbf{i} = (\xi_{x_i}, \xi_{p_i})^T$. The following holds

$$W^\dagger(\boldsymbol{\xi'}) W(\boldsymbol{\xi}) = e^{\frac{-i}{2}\boldsymbol{\xi'}^T \Omega \boldsymbol{\xi}} \hat{W}(\boldsymbol{\xi'} - \boldsymbol{\xi}), \tag{1.20}$$

[10] $W(\boldsymbol{\xi}) = W(\boldsymbol{\xi}) \cdot \mathbb{1} = W(\boldsymbol{\xi}) \int_{-\infty}^{\infty} |x\rangle \langle x| \, dx = \int_{-\infty}^{\infty} e^{-i\xi_x x} \left| x + \frac{\xi_p}{2} \right\rangle \left\langle x - \frac{\xi_p}{2} \right| dx$

where Ω_N is the *symplectic matrix*. The Wigner fuction $W(\mathbf{r})$ for N modes is equal to

$$\frac{1}{(2\pi)^{2N}}\int_{\mathbb{R}^{2N}} e^{i\sum_{i=1}^{N} x_i' p_i} \left\langle x_1 - \frac{x_1'}{2}\right| ... \left\langle x_N - \frac{x_N'}{2}\right| \rho \left| x_1 + \frac{x_1'}{2}\right\rangle ... \left| x_N + \frac{x_N'}{2}\right\rangle dx_1'...dx_N'. \tag{1.21}$$

Gaussian states can be defined as states possessing a Gaussian Wigner function

$$W_{Gauss}(\mathbf{r}) = \frac{e^{-(\mathbf{r}-\mathbf{d})^T\gamma^{-1}(\mathbf{r}-\mathbf{d})}}{\pi^N\sqrt{\det(\gamma)}} \tag{1.22}$$

and the corresponding characteristic function is of the form

$$C_{Gauss}(\boldsymbol{\xi}) = e^{-\frac{1}{4}\boldsymbol{\xi}^T\gamma\boldsymbol{\xi} - i\boldsymbol{\xi}^T\mathbf{d}}, \tag{1.23}$$

where γ is the so-called *covariance matrix* (CM), also called the matrix of second moments, and vector $\mathbf{d}$ is so-called *vector of first moments*. The covariance matrix γ has elements

$$\gamma_{ij} = \langle\{\Delta r_i, \Delta r_j\}\rangle = \mathrm{Tr}[\rho\{\Delta r_i, \Delta r_j\}] = \langle r_i r_j + r_j r_i\rangle - 2\langle r_i\rangle\langle r_j\rangle \tag{1.24}$$

and vector $\mathbf{d}$ is defined as $d_i = \langle r_i\rangle = \mathrm{Tr}[\rho\, r_\mathbf{i}]$. For a single mode, γ and $\mathbf{d}$ would be as follows

$$\gamma = \begin{pmatrix} 2\langle(\Delta x)^2\rangle & \langle\{\Delta x, \Delta p\}\rangle \\ \langle\{\Delta x, \Delta p\}\rangle & 2\langle(\Delta p)^2\rangle \end{pmatrix}, \mathbf{d} = \begin{pmatrix}\langle x\rangle \\ \langle p\rangle\end{pmatrix}. \tag{1.25}$$

The Gaussian state is completely described by a vector of first moments $\mathbf{d}$ and a covariance matrix γ, however, other states are not. A CM must be bounded in some way in order to be a physical CM. More precisely, it must satisfy the uncertainty relation [21]

$$\gamma + i\Omega_N \geq 0. \tag{1.26}$$

CM γ of any N-mode CV state must satisfy this inequality. Note that the inequality implies $\gamma > 0$ and conversely, it means that in order for a real symmetrical and strictly positive $2N \times 2N$ matrix to be a CM of a physical quantum state it must satisfy inequality (1.26).

1.2 Quantum steering

Let us now focus on the definition of the main concept of this thesis[11]. A definition similar to what can be found in [4, 22, 23] will be given here. Before giving a proper definition, let us remind ourselves what steering is. Considering the bipartite case, i.e. two parties, we ask whether it is possible for Alice, by her choice of measurement, to be able to collapse Bob's system into a different state.

Two parties, Alice and Bob, share an entangled quantum state ρ_{AB}. Alice can perform various measurements, selecting different measurement settings X and getting the results a. We denote the set of measurements which Alice can perform by $\mathcal{M}_A$. For each setting X and result a, Bob will have the unnormalized conditional state $\rho_B^{(a)}$ from a corresponding ensemble $\mathcal{E}^X = \{\rho_B^{(a)} : a \in \sigma(X)\}$ and the conditional states should be of the form

$$\rho_B^{(a)} = \mathrm{Tr}_A[\rho_{AB}(\hat{\Pi}_a^X \otimes \mathbb{1}_B)], \tag{1.27}$$

[11] An operational definition of steering is provided in [5] (page 3, left column).

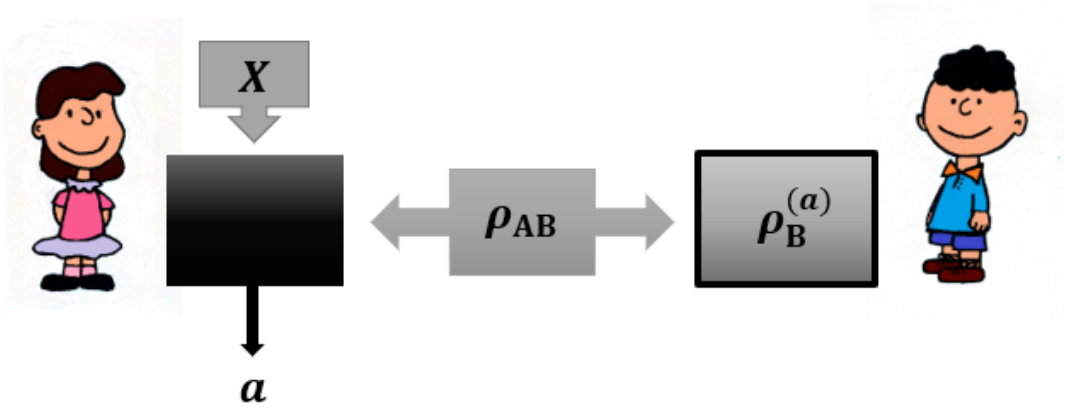

Figure 1.3: Alice and Bob demonstrating quantum steering. Alice is performing measurement with setting X and result a. Alice's device is untrusted (represented by a black box), while Bob uses principles of quantum mechanics to describe measurements and is trustworthy.

where $\hat{\Pi}_a^X$ is the POVM element corresponding to a measurement of the observable X and the result a. The set of all Bob's conditional states is known as the *steering assemblage* and it holds that $\rho_B = \sum_a \rho_B^{(a)}$. Note that Bob's unconditional state $\rho_B = \mathrm{Tr}[\rho_{AB}]$ does not depend on Alice's choice of measurement. In addition, Bob believes that the results of the measurements can be described by quantum mechanics and he does not trust Alice. Before starting the measurements, Bob asks Alice to announce into which ensembles $\{\mathcal{E}^X : X \in \mathcal{M}_A\}$ she can steer his state. Bob randomly selects one of these ensembles $\mathcal{E}^X$ and asks Alice to prepare it, which she does by measuring X on her subsystem. She then tells Bob the result of the measurement a, which allows Bob to predict which state $\rho_B^{(a)}$ he has. After many repetitions, they can verify that the states $\rho_B^{(a)}$ are indeed produced.

Bob can try to explain what has happened in the following way: He might assume that at the beginning, his system was in some local-hidden state σ_B^λ with the probability $p(\lambda)$. This state would be pulled from a pre-existing ensemble of LHSs $\mathcal{E}^{LHS} = \{p(\lambda)\sigma_B^\lambda\}$. In that case, Alice's measurement of X and the result a would only give Bob additional information about the probability of the conditional states, giving him states of the form [4, 23][12]

$$\rho_B^{(a)} = p(a|X) \int d\lambda\, p(\lambda|a, X)\sigma_B^\lambda = \int d\lambda\, p(\lambda)p(a|X, \lambda)\sigma_B^\lambda. \tag{1.28}$$

Both of these two equal expressions have different interpretations. The first expression tells us that the probability $p(\lambda|a, X)$ is a Bayesian update[13] of the probability $p(\lambda)$ after announcing the measurement setting X and the outcome a. Thus, Bob does not have to believe that Alice can control his state since the measurement and its outcome only gave Bob additional information about the distribution of the states σ_B^λ.

[12]The setting X is independent of λ and can be chosen at will, i.e. $p(X,\lambda) = p(X)p(\lambda)$. We can prove the equality: $p(\lambda|a, X) = \frac{p(\lambda,a,X)}{p(a,X)} = \frac{p(a|X,\lambda)p(X,\lambda)}{p(a|X)p(X)} = \frac{p(a|X,\lambda)p(X)p(\lambda)}{p(a|X)p(X)} = \frac{p(a|X,\lambda)p(\lambda)}{p(a|X)}$.

[13]We can write Bayes' theorem in the following way: $p(\lambda|a, X) = \frac{p(\lambda)p(a, X|\lambda)}{p(a, X)}$ when measuring X and getting the result a. If we do a Bayesian update then upon measuring X and getting a new result a', the initial prior probability $p(\lambda)$ will be equal to the old posterior probability $p(\lambda|a, X)$, i.e. $p(\lambda) = p(\lambda|a, X)$.

The second expression tells us that Alice can try to fool Bob by simulating his conditional states $\rho_B^{(a)}$ by pulling out the states σ_B^{λ} according to the distribution $p(\lambda)$ while reporting the results a depending on her knowledge of the measurement setting X and the parameter λ. However, Bob may not believe that the shared initial state was entangled.

To summarize, if there is a model as in Eq. (1.28), then Bob does not need to consider that Alice can control his state to explain the conditional states $\rho_B^{(a)}$. This state has a so-called local-hidden-state (LHS) model and is thus *unsteerable*. However, if there is no such model, then Bob must accept that Alice is able to influence his state, i.e. she is able to steer his state and therefore this state is *steerable*.

We can show that there are states in which Alice can steer Bob, but not vice versa. Hence steering is an asymmetric correlation. When Alice steers Bob, we denote it $A \to B$ and when Bob steers Alice, we denote it $B \to A$. If Alice can steer Bob and Bob can steer Alice, then we denote it $A \leftrightarrow B$. Let us now simply define the following: If $A \to B$ or $B \to A$ then the state is one-way steerable, but if $A \to B$ and $B \to A$ ($A \leftrightarrow B$) then the state is two-way steerable.

So far we have only talked about bipartite steering, now let us define *tripartite steering*. We consider three systems 1, 2, 3, and a bipartite split $1|23$[14]. A state is steerable in the direction $23 \to 1$ if it cannot be written as

$$\rho^{(23)} \equiv \rho_{23\to 1}^{uns} \equiv \sum_i \lambda_i \rho_{1,\,Q}^{(i)} \otimes \rho_{23}^{(i)}, \tag{1.29}$$

where λ_i are probabilities. If we are dealing with steering in the direction $23 \to 1$, then this state is steerable if it cannot be written as the state $\rho^{(23)}$. Analogously, we will denote states that are steerable in the opposite direction or different bipartition, e.g. $\rho_{1\to 23}^{uns} = \rho^{(1)}$ or $\rho_{12\to 3}^{uns} = \rho^{(12)}$. This allows us to implement even more generic notation. We introduce the set of all subsystems $\mathcal{S} = \{1, 2, 3, 12, 23, 13\}$, now we can denote some general unsteerable state $\rho^{(i)}$, $s \in \mathcal{S}$. The index Q in $\rho_{1,\,Q}^{(i)}$ indicates that the subsystem 1 is trusted and uses quantum mechanics, while the other subsystem is untrusted. So, e.g. for $\rho^{(23)}$ the subsystem 23 is untrusted while the other subsystem 1 is trusted.

Let us now define the so-called *genuine tripartite steering* (GTS). A state is one-way GTS if it cannot be expressed as

$$\rho_{\to}^{GMS} \neq \sum_{s\in\mathcal{S}} \lambda_s \rho^{(s)}, \tag{1.30}$$

where λ_s are probabilities. To be able to easily define two-way GTS, we need to introduce a slightly different notation. When discussing two-way tripartite steering, we have three possibilities for how to perform it: $1 \leftrightarrow 23$, $2 \leftrightarrow 13$, and $3 \leftrightarrow 12$. They can be thought of as a set of ordered pairs $\mathcal{B} = \{(1, 23), (2, 13), (3, 12)\}$. We can say the state is two-way steerable if we cannot write it as $\rho_b^{uns} = \rho^{(b)}$, e.g. $\rho_{1\leftrightarrow 23}^{uns} = \rho^{(1\leftrightarrow 23)}$. Then a state is two-way GTS if it cannot be expressed as

$$\rho_{\leftrightarrow}^{GMS} \neq \sum_{b\in\mathcal{B}} \lambda_\beta \rho^{(b)}. \tag{1.31}$$

[14]The notation $1|23$ means that it is not specified whether the steering is two-way or one-way nor in which direction, but it tells us that we are working with the two specific sides.

It is generally difficult to construct a LHS model for a given quantum state. Therefore, various steering criteria have been developed. The criteria typically have the form of a multi-mode uncertainty relation involving second-order moments of quadrature operators. In this thesis, we examine such criteria for the three-mode generalization of steering. Such criteria already appeared in the literature. For example, a widely used criterion of Reid and co-workers [16] is of the following form:

$$\begin{aligned} &\Delta(h_1x_1 + h_2x_2 + h_3x_3)\Delta(g_1p_1 + g_2p_2 + g_3p_3) \\ &\geq min\{|g_1h_1|,|g_2h_2 + g_3h_3|,|g_2h_2|,|g_1h_1 + g_3h_3|,|g_3h_3|,|g_1h_1 + g_2h_2|,\} \end{aligned} \tag{1.32}$$

where ΔA denotes standard deviation of quadrature operators x_i or p_i, h_i, $g_i \in \mathbb{R}$. If the inequality is violated, then the state is GTS. Obviously, the standard deviations Δu and Δv use the whole CM. A natural question arises as to whether an even simpler criterion can be derived. In this thesis, we answer this question in the affirmative by deriving a minimal criterion for GTS.

Chapter 2

Results

This chapter contains the original results of this thesis. Specifically, we derive the anticipated minimal criterion and then show that it is applicable by detecting several GTS states.

2.1 Criterion

We are going to seek the so-called minimal criterion for genuine three-mode steering. The term "minimal" implies that the criterion does not need the knowledge of the entire covariance matrix for detection. However, before we proceed to the actual derivation, we will add a brief and simple explanation of what we require the minimal criterion to fulfill.

2.1.1 Preliminaries for the minimal criterion

We look for a criterion that will satisfy the following two requirements:

1. It will use the least number of two-mode reduced CMs.
2. It will contain the minimum possible number of at most two-mode combinations of the quadrature operators.

Let us consider a state of three modes 1, 2 and 3 with CM

$$\gamma_{123} = \begin{pmatrix} \gamma_1 & \omega_{12} & \omega_{13} \\ \omega_{12}^T & \gamma_2 & \omega_{23} \\ \omega_{13}^T & \omega_{23}^T & \gamma_3 \end{pmatrix}. \tag{2.1}$$

We are interested in criteria that do not require knowledge of the entire CM. The whole matrix is contained in all three marginals γ_{12}, γ_{23} and γ_{13}, whereas we only want to use the least number of marginals that suffice for the detection of steering. The respective set of marginal CMs is called a *minimal set* and for three modes it is given by, e.g. $\{\gamma_{12}, \gamma_{23}\}$. Here we took inspiration from Ref. [24] as well as Ref. [25] where analogous criteria were derived for the detection of genuine multipartite entanglement (GME). To detect GME the minimal set of marginal CMs has to contain all modes and the marginals have to overlap. The same must hold for GTS and so the marginal CMs are of the following form

$$\gamma_{12} = \begin{pmatrix} \gamma_1 & \omega_{12} \\ \omega_{12}^T & \gamma_2 \end{pmatrix}, \gamma_{23} = \begin{pmatrix} \gamma_2 & \omega_{23} \\ \omega_{23}^T & \gamma_3 \end{pmatrix}. \tag{2.2}$$

The minimal set can conveniently be represented by a special sort of graph known as a tree (see Fig. 2.1).

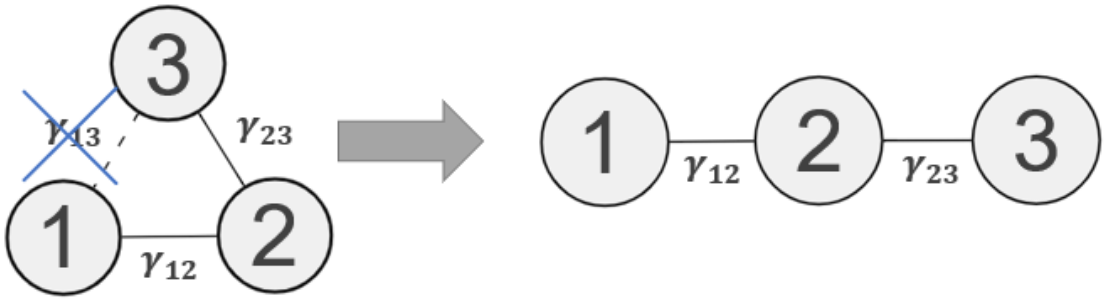

Figure 2.1: The figure on the left is a complete tree with three vertices representing a complete set of two-mode marginals CMs $\{\gamma_{12}, \gamma_{23}, \gamma_{13}\}$ of all three modes described by full CM γ_{123}. Figure on the right represents the minimal set $\{\gamma_{12}, \gamma_{23}\}$ which is equivalent with knowledge of the entire CM γ_{123}.

2.1.2 Derivation of the criterion

The structure of the criterion can be found using a steering witness Z. As GME states [26], GMS states also form a closed convex set, therefore they can be separated using a real symmetric positive-semidefinite matrix Z. The separation can be executed by a hyperplane $\mathrm{Tr}[Z\gamma] = 0$.

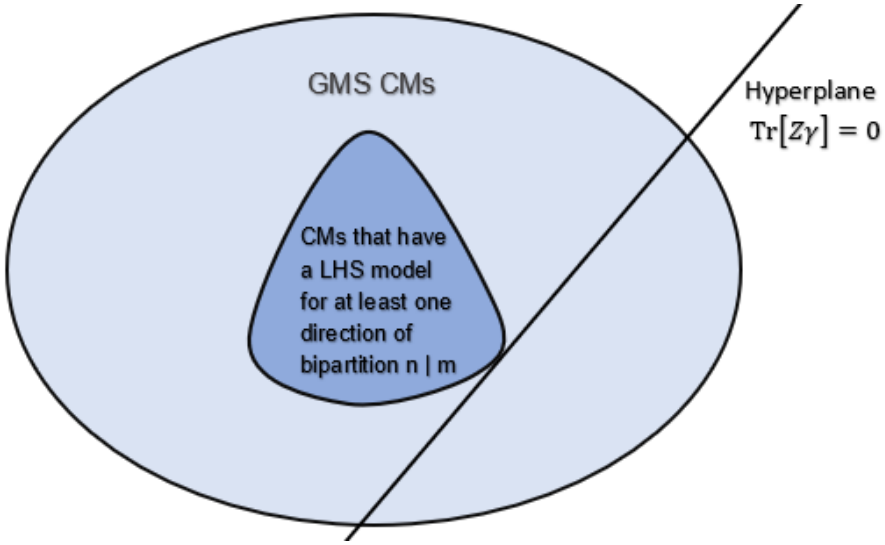

Figure 2.2: An image that graphically defines the role of a steering witness Z. By the bipartition $n|m$ we mean an arbitrary biparition 1|23, 2|13 or 3|12 for GTS states.

We assume for simplicity a block-diagonal witness matrix

$$Z = Z^x \oplus Z^p. \tag{2.3}$$

It can be shown that one can write

$$Z^{\alpha} = l^{\alpha}(l^{\alpha})^{T},\ \alpha = x,\ p, \tag{2.4}$$

where l^{α} is a lower triangular matrix with strictly positive real diagonal elements. It is not difficult to show that

$$Tr[Z^{\alpha}\gamma^{\alpha}] = \mathrm{Tr}[l^{\alpha}(l^{\alpha})^{T}\gamma^{\alpha}] = 2\sum_{i=1}^{3}\langle\{\Delta[(l^{\alpha})^{T}\boldsymbol{\xi^{\alpha}}]\}^{2}\rangle = 2\sum_{i=1}^{3}\langle(\Delta u_{i}^{\alpha})^{2}\rangle = 2U^{\alpha} \tag{2.5}$$

where $\boldsymbol{\xi^{\alpha}} = (\alpha_1,\ \alpha_2,\ \alpha_3)^{T}$ and $u_{i}^{\alpha} = \sum_{j=1}^{3} l_{ji}^{\alpha}\alpha_{j}$. The decompositions of Z in Eq. (2.4) is the so-called Cholesky decomposition [27]. The two requirements that were mentioned in the preliminaries were achieved by considering a *partially-blind witness*

$$Z^{\alpha} = \begin{pmatrix} Z_{1}^{\alpha} & Z_{12}^{\alpha} & \mathbf{0} \\ Z_{12}^{\alpha} & Z_{2}^{\alpha} & Z_{21}^{\alpha} \\ \mathbf{0} & Z_{23}^{\alpha} & Z_{3}^{\alpha} \end{pmatrix} \Rightarrow l^{\alpha} = \begin{pmatrix} l_{1}^{\alpha} & 0 & 0 \\ l_{21}^{\alpha} & l_{2}^{\alpha} & 0 \\ \mathbf{0} & l_{32}^{\alpha} & l_{3}^{\alpha} \end{pmatrix}. \tag{2.6}$$

With the new zero in l^{α} representing the missing block ω_{13}, all three-mode combinations of quadratures disappear and we get only at most two-mode combinations of quadrature operators as can be seen in

$$\begin{gathered} u_{1}^{x} = l_{11}^{x}x_1 + l_{21}^{x}x_2,\ u_{2}^{x} = l_{22}^{x}x_2 + l_{32}^{x}x_3,\ u_{3}^{x} = l_{33}^{x}x_3, \\ u_{1}^{p} = l_{11}^{p}p_1 + l_{21}^{p}p_2,\ u_{2}^{p} = l_{22}^{p}p_2 + l_{32}^{p}p_3,\ u_{3}^{p} = l_{33}^{p}p_3. \end{gathered} \tag{2.7}$$

The quadrature combinations can be conveniently derived directly from a graph (see Fig. 2.3).

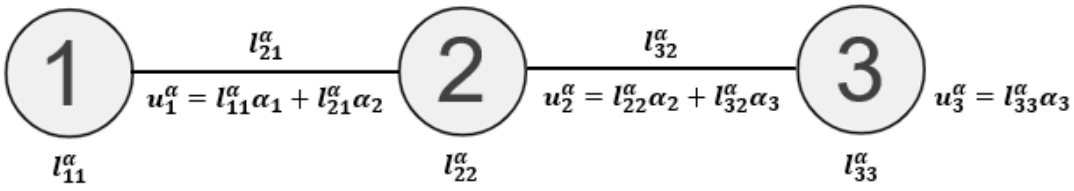

Figure 2.3: A graph of the interaction of three modes, where $\alpha = x,\ p$.

We will search for a criterion in the form of the product condition

$$U^{x}U^{p} \geq f(l^{x},\ l^{p}), \tag{2.8}$$

where $f(l^{x},\ l^{p})$ is some function of the elements of the matrices l^{α} from Cholesky decomposition of the steering witness and $U^{\alpha} = \sum_{i=1}^{3}\langle(\Delta u_{i}^{\alpha})^{2}\rangle$, $i = 1,\ 2,\ 3$, as defined in (2.5). Thus we get the quantities U^{x} and U^{p} that form the left-hand side (LHS) of the investigated criterion.

RHS of the criterion

Moving to the derivation of the right-hand side (RHS) of the criterion. We will find the RHS by finding a lower bound on $U^{x}U^{p}$ for a tripartite steerable state (1.30) or (1.31). Consider now three CV systems 1, 2, 3. First, we will find the lower bound for

bipartite split 1|23. We say that the state is $32 \to 1$ steerable if it cannot be written as $\rho^{(23)}$, Eq. (1.29). We first find the lower bound for the general operators

$$\begin{aligned} u^x &= l_1^x x_1 + l_2^x x_2 + l_3^x x_3, \\ u^p &= l_1^p p_1 + l_2^p p_2 + l_3^p p_3. \end{aligned} \tag{2.9}$$

The derivation is as follows

$$\langle (\Delta u^x)^2 \rangle_{\rho^{(23)}} \langle (\Delta u^p)^2 \rangle_{\rho^{(23)}} \overset{1}{\geq} \sum_i p_i \langle (\Delta u^x)^2 \rangle_{\rho_{1,\,Q}^{(i)} \otimes \rho_{23}^{(i)}} \sum_j p_j \langle (\Delta u^p)^2 \rangle_{\rho_{1,\,Q}^{(j)} \otimes \rho_{23}^{(j)}} \tag{2.10}$$

$$\begin{aligned} \overset{2}{\geq} \{ \sum_i p_i \sqrt{\langle [\Delta(l_1^x x_1)]^2 \rangle_{\rho_{1,\,Q}^{(i)}} + \langle [\Delta(l_2^x x_2 + l_3^x x_3)]^2 \rangle_{\rho_{23}^{(i)}}} \cdot \\ \cdot \sqrt{\langle [\Delta(l_1^p p_1)]^2 \rangle_{\rho_{1,\,Q}^{(i)}} + \langle [\Delta(l_2^p p_2 + l_3^p p_3)]^2 \rangle_{\rho_{23}^{(i)}}} \}^2 \end{aligned} \tag{2.11}$$

$$\begin{aligned} \overset{3}{\geq} | \sqrt{\langle [\Delta(l_1^x x_1)]^2 \rangle_{\rho_{1,\,Q}^{(i)}} \langle [\Delta(l_1^p p_1)]^2 \rangle_{\rho_{1,\,Q}^{(i)}}} + \\ + \sqrt{\langle [\Delta(l_2^x x_2 + l_3^x x_3)]^2 \rangle_{\rho_{23}^{(i)}} \langle [\Delta(l_2^p p_2 + l_3^p p_3)]^2 \rangle_{\rho_{23}^{(i)}}} |^2 \overset{4}{\geq} \frac{1}{4} |l_1^x l_1^p|^2 \end{aligned} \tag{2.12}$$

Where inequality 1 follows from the concavity of variance [28] (see Appendix 2), inequality 2 was obtained by assuming that it is a product of two norms and then using the Cauchy-Schwarz inequality. Inequality 3 again follows from Cauchy-Schwarz inequality and to get the last inequality 4 we used the following relations

$$\begin{aligned} \langle [\Delta(l_1^x x_1)]^2 \rangle \langle [\Delta(l_1^p p_1)]^2 \rangle &\geq \frac{1}{4} |l_1^x l_1^p|^2, \\ \langle [\Delta(l_2^x x_2 + l_3^x x_3)]^2 \rangle \langle [\Delta(l_2^p p_2 + l_3^p p_3)]^2 \rangle &\geq 0. \end{aligned} \tag{2.13}$$

Note that the second inequality is bound only by zero, this is because 23 is an untrusted system and thus we don't know if it is a quantum system, all we can say is that it is greater than zero, which distinguishes it from the lower bound for the GME criterion. Repeating the same argumentation for the other steering directions we get the lower bounds summarized in Tab. 2.1.

direction	**lower bound**
$23 \to 1$	$\geq \frac{1}{4} \lvert l_1^x l_1^p \rvert^2$
$12 \to 3$	$\geq \frac{1}{4} \lvert l_3^x l_3^p \rvert^2$
$13 \to 2$	$\geq \frac{1}{4} \lvert l_2^x l_2^p \rvert^2$
$1 \to 23$	$\geq \frac{1}{4} \lvert l_2^x l_2^p + l_3^x l_3^p \rvert^2$
$3 \to 12$	$\geq \frac{1}{4} \lvert l_1^x l_1^p + l_2^x l_2^p \rvert^2$
$2 \to 13$	$\geq \frac{1}{4} \lvert l_1^x l_1^p + l_3^x l_3^p \rvert^2$

Table 2.1: Table of lower bounds for all different steering bipartitions and directions.

Summarizing previous results we see that a given three-mode state ρ_{123} is $23 \to 1$ steerable, if it violates the following inequality

$$\langle (\Delta u^x)^2 \rangle_{(23)} \langle (\Delta u^p)^2 \rangle_{(23)} \geq \sum_i p_i (\Delta u^x)_i (\Delta u^p)_i \geq \sum_i p_i (\Delta u^x)_{1,\,Q} (\Delta u^p)_{1,\,Q} \geq C_1^{1|23}, \tag{2.14}$$

where $C_1^{1|23}$ represents the lower bound and the notation $C_1^{1|23}$ means that $23 \to 1$ and therefore that we consider split $1|23$ and the trusted system is system 1. We generalize this notation for a general bipartite split and direction. Recall that in Section 1.2 we introduced the set of ordered pairs $\mathcal{B}$. We can also use it as a set of all bipartite splits $\mathcal{B} = \{(1|23), (2|13), (3|12)\} = \{\beta_1, \beta_2, \beta_2\}$, i.e. its elements will be $\beta_i \in \mathcal{B}$, $i = 1, 2, 3$. If we take β_1, then we are dealing with the split $1|23$ and thus the trusted subsystem can be either subsystem 1 or 23 depending on the steering direction. We denote I if the trusted subsystem is 1 and II if it is 23, then for some general bipartite split β_i we have I = 1, 2 or 3 and II = 13, 13 or 12. From now on we will use the following identification: $C_I^{\beta_1} = C_1^{1|23}$, $C_{II}^{\beta_1} = C_{23}^{1|23}$ and so on.

The state ρ_{123} is *one-way tripartite steerable* in the bipartite split $\beta_i \in \mathcal{B}$ (in arbitrary direction) if the inequality

$$\langle(\Delta u^x)^2\rangle_{\beta_i}\langle(\Delta u^p)^2\rangle_{\beta_i} \geq \max\{C_{II}^{\beta_i}, C_I^{\beta_i}\} \tag{2.15}$$

is violated, i.e. if it is steerable in one arbitrary direction. The state ρ_{123} is *two-way tripartite steerable* in the bipartite split $\beta_i \in \mathcal{B}$ if the inequality

$$\langle(\Delta u^x)^2\rangle_{\beta_i}\langle(\Delta u^p)^2\rangle_{\beta_i} \geq \min\{C_{II}^{\beta_i}, C_I^{\beta_i}\} \tag{2.16}$$

is violated, i.e. if it is steerable in both directions. Now, the state ρ_{123} will be *one-way GTS* if the following inequality

$$\langle(\Delta u^x)^2\rangle\langle(\Delta u^p)^2\rangle \geq \sum_{\beta_i\in\mathcal{B}} \lambda_{\beta_i}\max\{C_{II}^{\beta_i}, C_I^{\beta_i}\} \geq \min_{\beta_i} \max\{C_{II}^{\beta_i}, C_I^{\beta_i}\} \tag{2.17}$$

is violated. And the state ρ_{123} is *two-way GTS* if inequality

$$\langle(\Delta u^x)^2\rangle\langle(\Delta u^p)^2\rangle \geq \sum_{\beta_i\in\mathcal{B}} \lambda_{\beta_i}\max\{C_{II}^{\beta_i}, C_I^{\beta_i}\} \geq \min_{\beta_i} \min\{C_{II}^{\beta_i}, C_I^{\beta_i}\} \tag{2.18}$$

is violated.

Let us now return to our minimal criterion. The LHS of our criterion is

$$U^x U^p = \sum_{i,j}^{3} \langle(\Delta u_i^x)^2\rangle\langle(\Delta u_j^p)^2\rangle, \tag{2.19}$$

where u_i^x and u_j^p are operators defined in Eq. (2.7). This gives us the sum of nine expressions $\langle(\Delta u_i^x)^2\rangle\langle(\Delta u_j^p)^2\rangle$, i, $j = 1, 2, 3$ that have a lower bound for each of the bipartite splits

$$\begin{aligned} U^x U^p = \langle[\Delta(l_{11}^x x_1 + l_{21}^x x_2)]^2\rangle\langle[\Delta(l_{11}^p p_1 + l_{21}^p p_2)]^2\rangle + \langle[\Delta(l_{11}^x x_1 + l_{21}^x x_2)]^2\rangle\cdot \\ \cdot\langle[\Delta(l_{22}^p p_2 + l_{32}^p p_3)]^2\rangle + \langle[\Delta(l_{11}^x x_1 + l_{21}^x x_2)]^2\rangle\langle[\Delta(l_{33}^p p_3)]^2\rangle + \dots . \end{aligned} \tag{2.20}$$

The lower bounds are summarized in Tab. 2.2.

expression	$\boldsymbol{\beta_1}$		$\boldsymbol{\beta_2}$		$\boldsymbol{\beta_3}$	
E_{ij}	C_{II}	C_I	C_{II}	C_I	C_{II}	C_I
$i=1,\, j=1$	$(l^x_{11}l^p_{11})^2$	$(l^x_{21}l^p_{21})^2$	$(l^x_{21}l^p_{21})^2$	$(l^x_{11}l^p_{11})^2$	0	$(l^x_{11}l^p_{11}+l^x_{21}l^p_{21})^2$
$i=1,\, j=2$	0	$(l^x_{21}l^p_{22})^2$	$(l^x_{21}l^p_{22})^2$	0	0	$(l^x_{21}l^p_{22})^2$
$i=1,\, j=3$	0	0	0	0	0	0
$i=2,\, j=1$	0	$(l^x_{22}l^p_{21})^2$	$(l^x_{22}l^p_{21})^2$	0	0	$(l^x_{22}l^p_{21})^2$
$i=2,\, j=2$	0	$(l^x_{22}l^p_{22}+l^x_{32}l^p_{32})^2$	$(l^x_{22}l^p_{22})^2$	$(l^x_{32}l^p_{32})^2$	$(l^x_{32}l^p_{32})^2$	$(l^x_{22}l^p_{22})^2$
$i=2,\, j=3$	0	$(l^x_{32}l^p_{33})^2$	0	$(l^x_{32}l^p_{33})^2$	$(l^x_{32}l^p_{33})^2$	0
$i=3,\, j=1$	0	0	0	0	0	0
$i=3,\, j=2$	0	$(l^x_{33}l^p_{32})^2$	0	$(l^x_{33}l^p_{32})^2$	$(l^x_{33}l^p_{32})^2$	0
$i=3,\, j=3$	0	$(l^x_{33}l^p_{33})^2$	0	$(l^x_{33}l^p_{33})^2$	$(l^x_{33}l^p_{33})^2$	0

Table 2.2: Table of all lower bounds for all nine expressions $E_{ij} = 4\langle(\Delta u^x_i)^2\rangle\langle(\Delta u^p_j)^2\rangle$ for all bipartite splits $\{\beta_1, \beta_2, \beta_2\} = \{(1|23), (2|13), (3|12)\}$.

Let us introduce the quantities $\mathcal{L}^{\beta_i}_I$ and $\mathcal{L}^{\beta_i}_{II}$ which will be equal to the sum of the individual columns in the Tab. 2.2, e.g.

$$\mathcal{L}^{\beta_i}_{II} = (l^x_{11}l^p_{11})^2,$$

$$\mathcal{L}^{\beta_i}_{I} = (l^x_{21}l^p_{21})^2 + (l^x_{21}l^p_{22})^2 + (l^x_{22}l^p_{21})^2 + (l^x_{22}l^p_{22}+l^x_{32}l^p_{32})^2 + (l^x_{32}l^p_{33})^2 + (l^x_{33}l^p_{32})^2 + (l^x_{33}l^p_{33})^2,$$

and so on. We can now finally write down the final form of our criterion. The state ρ_{123} is *one-way GTS* if the inequality

$$U^xU^p \geq \frac{1}{4}\min\{\max[\mathcal{L}^{\beta_1}_I, \mathcal{L}^{\beta_1}_{II}], \max[\mathcal{L}^{\beta_2}_I, \mathcal{L}^{\beta_2}_{II}], \max[\mathcal{L}^{\beta_3}_I, \mathcal{L}^{\beta_3}_{II}]\} \equiv \mathcal{R}_{\rightarrow} \tag{2.21}$$

is violated and the state is *two-way GTS* if the inequality

$$U^xU^p \geq \frac{1}{4}\min\{\min[\mathcal{L}^{\beta_1}_I, \mathcal{L}^{\beta_1}_{II}], \min[\mathcal{L}^{\beta_2}_I, \mathcal{L}^{\beta_2}_{II}], \min[\mathcal{L}^{\beta_3}_I, \mathcal{L}^{\beta_3}_{II}]\} \equiv \mathcal{R}_{\leftrightarrow} \tag{2.22}$$

is violated.

2.2 Detection of genuine multipartite steering

After deriving the criterion, the time has come to test it. Our task is to find states with GTS detectable by our minimal criterion. In this section, we will use the term steerable in the sense of genuine tripartite steerable.

2.2.1 Detection method

First, let us have a look at the detection method. We already know that by using CMs we can represent all correlations of Gaussian states, which we will utilize in this chapter. Prior to presenting the results in each section, we will always explain how we obtained the CMs. Allow us to mention once again that we do not need knowledge of the entire CM to apply our minimal criterion. Once we obtained a CM, we optimize our criterion over the parameters l^α_{ij} ($\alpha = x,\, p;\ i,\, j = 1,\, 2,\, 3$) to find the minimum value of the difference between LHS and RHS of the criterion. If this minimum is negative, then the state is steerable. For this difference we introduce the notation

$D_{\rightarrow} = U^x U^p - \mathcal{R}_{\rightarrow}$ for one-way steering and $D_{\leftrightarrow} = U^x U^p - \mathcal{R}_{\leftrightarrow}$ for two-way steering. In addition, for the sake of simplicity, the minimization of parameters l_{ij}^{α} was restricted to the interval $[-1,1]$. To improve the process of searching for the minima, we used an optimization method called RandomSearch method [29, 30], which works by generating a set of random initial points and using a local optimization method from each one of the initial points and then converges to a local minimum. The only problem is that it takes much longer to find the minimum when using the RandomSearch method.

To find steerable states, we used two methods to obtain CMs exhibiting GTS – random generation of numerical matrices and deriving them from a linear-optical scheme.

2.2.2 Numerical three-mode covariance matrices

In this subsection, we will analyze steering in a hundred "randomly" generated genuine tripartite entangled (GTE) CMs[1]. Tab. 2.3 shows the number of times steering was detected by our criterion for these CMs.

	one-way	**two-way**
Number of states	91	0

Table 2.3: Number of one-way and two-way steerable states detected by our criterion from 100 GTE CMs.

For illustration, we present and discuss one of these numerical CMs which reads explicitly as

$$\gamma_{num} = \begin{pmatrix} 4.88 & 0 & 10.76 & 0 & -16.66 & 0 \\ 0 & 6.59 & 0 & -11.55 & 0 & -5.60 \\ 10.76 & 0 & 28.15 & 0 & -45.42 & 0 \\ 0 & -11.55 & 0 & 23.45 & 0 & 11.77 \\ -16.66 & 0 & -45.42 & 0 & 74.15 & 0 \\ 0 & -5.60 & 0 & 11.77 & 0 & 5.97 \end{pmatrix}. \tag{2.23}$$

The matrix (refeqn:cmnum) is a CM obtained as follows: We rounded elements of a CM [2] to two decimal places. However, the rounded did not satisfy the uncertainty principle

$$\gamma_{num} + i\Omega_N \geq 0, \tag{2.24}$$

indicating that it was no longer a CM. We can correct the fact that the eigenvalues of the rounded matrix contained negative numbers by adding the smallest negative eigenvalue rounded to the appropriate number of decimal places (for us to two decimal places). Thus we get the matrix $\gamma_{num} + |\lambda| \cdot \mathbb{1}$, where $\lambda = \min Eig\{\gamma_{num} + i\Omega_N\}$.This matrix is our CM in Eq. (2.23) for which we have verified that all eigenvalues are positive. We then tested whether this CM violates our criterion, i.e. whether it is GTS CM. You can find the values of $D_{\rightarrow}$ and $D_{\leftrightarrow}$ in the Tab. 2.4.

$\boldsymbol{D_{\rightarrow}}$	$\boldsymbol{D_{\leftrightarrow}}$
$-1.8 \cdot 10^{-2}$	inconclusive

Table 2.4: Differences $D_{\rightarrow}$ and $D_{\leftrightarrow}$ CM (2.23). By the term inconclusive, we mean that it is not two-way steerable and $D_{\leftrightarrow}$ is so small (of order 10^{-18} and less) that it does not need to be specified.

[1] The procedure of generating these CMs is described in the article [25].

[2] See Appendix 3 for the original unrounded matrix

For the CM (2.23) we also include a table of values of the optimization parameters l_{ij}^{α} for one-way steering (see Tab. 2.5).

$\mathbf{l_{ij}^{x}}$	**Value**	$\mathbf{l_{ij}^{p}}$	**Value**
l_{11}^{x}	-1	l_{11}^{p}	1
l_{21}^{x}	0.375	l_{21}^{p}	0.492
l_{22}^{x}	0.769	l_{22}^{p}	-0.512
l_{32}^{x}	0.471	l_{32}^{p}	1
l_{33}^{x}	0.001	l_{32}^{p}	0.001

Table 2.5: The values of the optimization parameters l_{ij}^{α} rounded to three decimal places for the CM (2.23).

The values for l_{33}^{x} and l_{33}^{p} were 10^{-8} and 10^{-6} respectively and using these we obtained the difference $D_{\rightarrow} = -1.751 \cdot 10^{-2}$. To avoid having such small numbers in the table, we set these two values to 10^{-3} and then tested again how strongly would the CM violate our criterion. The result was $-1.749 \cdot 10^{-2}$, so we can see that changing such small parameters to larger ones (but still relatively small) hardly changes the violation. We then tried rounding the original matrix (3.11) to one decimal place and then repeated the process, but this CM no longer violated the criterion and thus is not a GTS.

2.2.3 General three-mode state

After discussing numerical CMs, we can move on to the derivation of analytical CMs violating our GTS criterion. In Fig. 2.4 we present the linear-optical scheme generating the states (see Appendix 4 for the derivation of CMs). The scheme produces five free parameters that we can optimize, which gives us the freedom to search for steerable states.

Now, the task is to find parameters from the scheme in Fig. 2.4 for which there would exist GTS states. All the different CMs given by the different parameters were tested for both one-way steering and two-way steering, but since none of the states were two-way steerable according to our criterion, we will not comment further on two-way steering. Thus, in the following, we will only discuss one-way steering and the respective difference will be simply denoted as $D_{\rightarrow} = D$.

Let us now move on to presenting the results. Tab. 2.6 contains the values of the parameters that define the different regions of the GTS states.

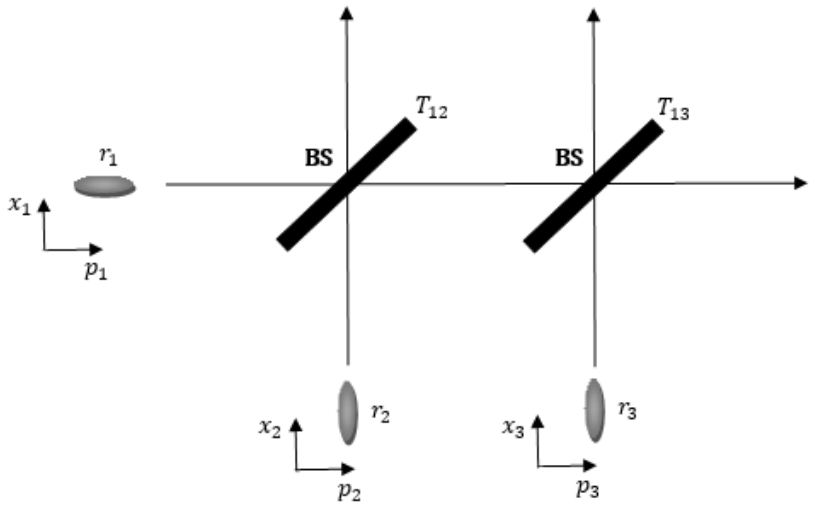

Figure 2.4: The linear-optical circuit consists of three squeezed-vacuum states (grey ellipses) with three different squeezing parameters r_1, r_2, r_3 and two beam splitters (black rectangles) with two different transmissivities T_{12}, T_{13}. The x_i and p_i are the two orthogonal quadrature operators of the three spatially separated optical modes. The depicted local coordinate systems p_i, x_i are used for indication of the orientation of the squeezing ellipses.

Region	$\mathbf{T_{12}}$	$\mathbf{T_{13}}$	$\mathbf{r_1}$	$\mathbf{r_2}$	$\mathbf{r_3}$
I	$\frac{2}{3}$	$\frac{1}{2}$	[1.0, 1.9]	[1.5, 2.0]	0.25
II	$\frac{11}{20}$	$\sqrt{\frac{2}{3}}$	[1.2, 2.0]	[1.4, 2.0]	0.10
III	$\frac{2}{3}$	$[\frac{1}{5}, \frac{7}{10}]$	1.30	1.50	[0.05, 0.40]
IV	$\sqrt{\frac{1}{2}}$	$[\frac{1}{5}, \frac{7}{10}]$	1.50	1.50	[0.05, 0.50]

Table 2.6: Table of parameters defining the three regions of GTS states. The parameters that are given by an interval are the free parameters over which we optimized the criterion. The step with which the free parameters were increasing was 0.05 and that's a step we will use throughout this section.

The parameters of the scheme with the strongest violation of the criterion for each region, i.e. with least D, are summarized in Tab. 2.7.

Region	$\mathbf{T_{12}}$	$\mathbf{T_{13}}$	$\mathbf{r_1}$	$\mathbf{r_2}$	$\mathbf{r_3}$	**D**
I	$\frac{2}{3}$	$\frac{1}{2}$	1.05	1.50	0.25	$-3.4 \cdot 10^{-2}$
II	$\frac{11}{20}$	$\sqrt{\frac{2}{3}}$	2.00	2.00	0.10	$-3.1 \cdot 10^{-2}$
III	$\frac{2}{3}$	$\frac{9}{20}$	1.30	1.50	0.15	$-1.1 \cdot 10^{-2}$
IV	$\sqrt{\frac{1}{2}}$	$\frac{1}{2}$	1.50	1.50	0.05	$-1.7 \cdot 10^{-2}$

Table 2.7: The parameters with the strongest violation of the criterion and corresponding D.

We have also depicted all these regions graphically. The graphs can be found in Figs. 2.5-2.8.

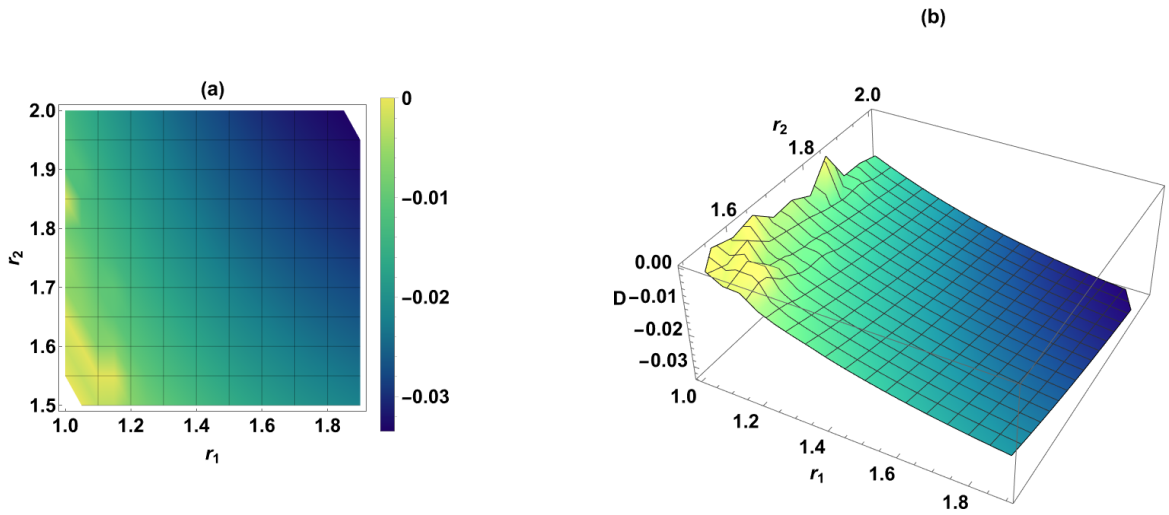

Figure 2.5: Dependence of the difference D on the squeezing parameters r_1 and r_2 for the region I.

From Fig. 2.5 one can see that this region is full of GTS states, i.e. states that violate our criterion. From Fig. (a) we see that the violation of the criterion reaches values over -0.03, which for us is so far the strongest observed violation of our criterion. It is evident from both figures that for increasing parameters r_1 and r_2 the difference D is decreasing, i.e., the violation of our criterion is becoming larger. The strongest distortion of our criterion occurred in this region.

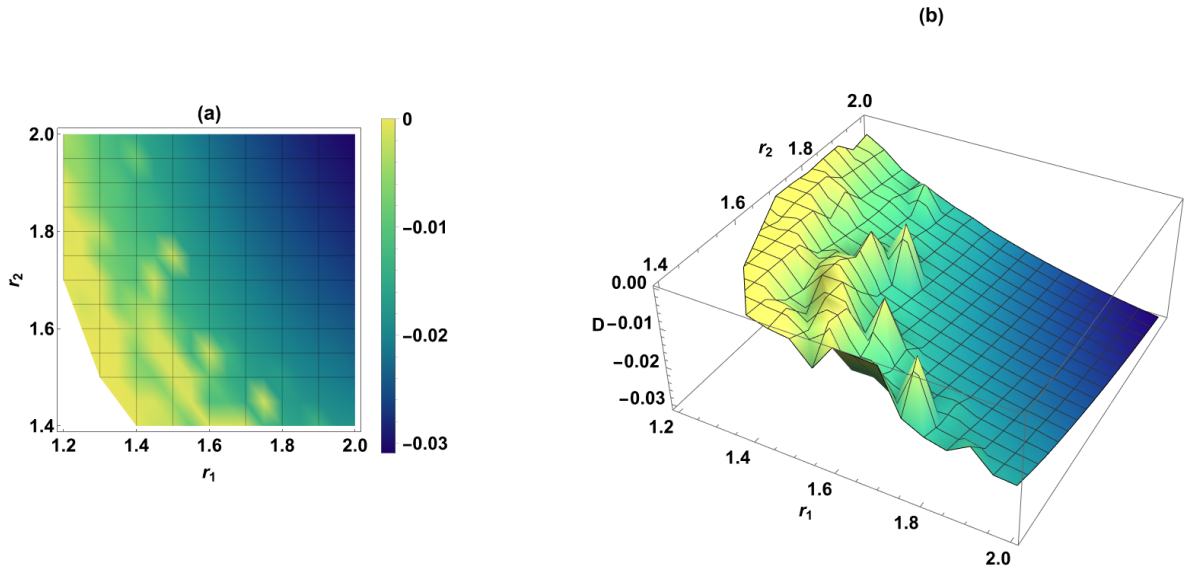

Figure 2.6: Dependence of the difference D on the squeezing parametres r_1 and r_2 for the region II.

In Fig. 2.6 we observe similar behavior as in Fig. 2.5. Although the transmissivity T_{12} and T_{13} and squeezing parameter r_3 are defined differently, we optimized over the same parameters r_1 and r_2 as in region I. In region I, however, there was only one unsteerable state, whereas in region II there are considerably more unsteerable states.

Moreover, the difference D does not go as low as in region I, which can also be seen from the table of the strongest violations (Tab. 2.7). Although it is not that low, it still reaches values over -0.03 in some locations.

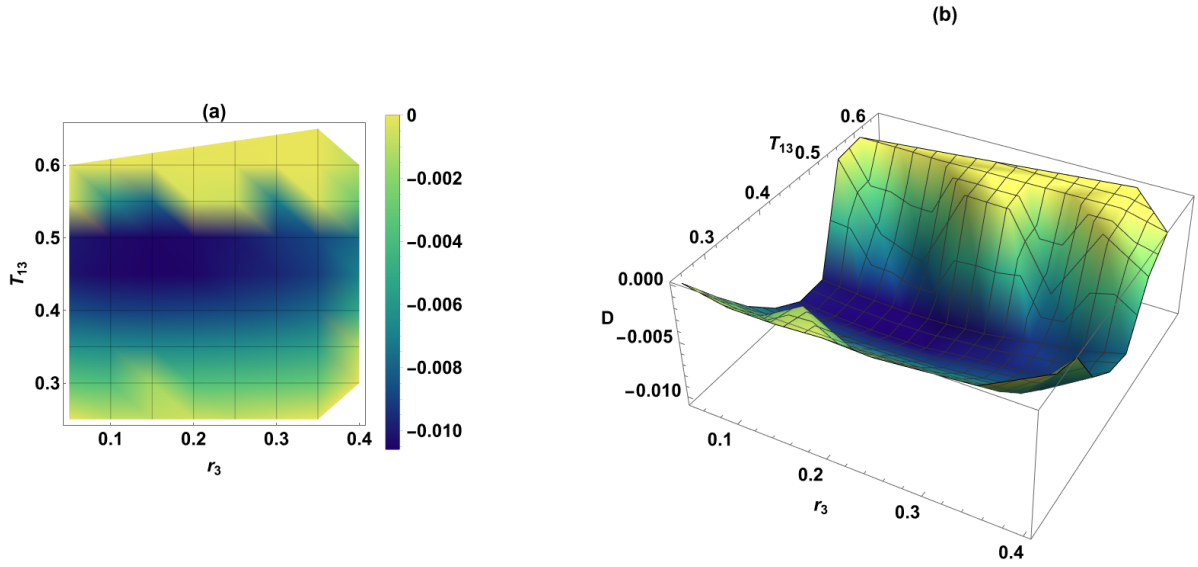

Figure 2.7: Dependence of the difference D on the squeezing parametres T_{13} and r_3 for the region III.

Fig. 2.7 depicts a completely different dependence than the previous two, as we optimized over different parameters. From graph (a) one can clearly see that the difference D only reached values slightly over -0.01, which is rather weak and it makes it the weakest of the four regions. The strongest violations of our criterion occurred for $T_{13} \in [0.4, 0.5]$.

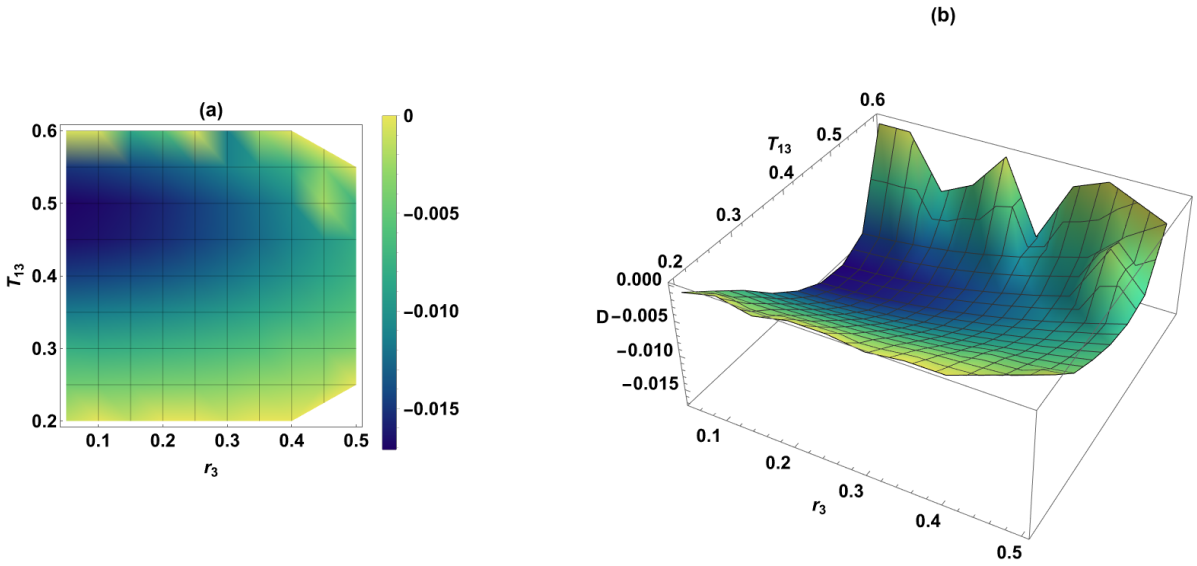

Figure 2.8: Dependence of the difference D on the squeezing parametres T_{13} and r_3 for the region IV.

Since we optimized over the same two parameters, region IV in Fig. 2.8 resembles

region III. In this region, however, we achieved lower differences D compared to Region III. The strongest violations and thus lowest differences D were observed for $T_{13} \in [0.4, 0.55]$ and $r_3 \in [0.05, 0.2]$.

Chapter 3

Conclusion

One could say that the minimal criteria for genuine multipartite steering form a gap in this field of research. Therefore, in this thesis, we have derived such a criterion for detecting genuine tripartite steering. Our criterion is a so-called minimal criterion, more precisely it does not require knowledge of the entire covariance matrix. Our criterion was not designed for a specific state, but for searching for GTS states. We have demonstrated that our criterion is able to detect these states by finding multiple regions of GTS states. However, several questions remain open. These include two-way steering and finding of a state exhibiting a stronger violation of the presented criterion, generalization of the criterion to more than three modes, and exploration of the possibility to find a partially blind steering witness using positive-semidefinite programming. Another interesting question is whether one may also have a Gaussian state whose genuine multipartite steering can be detected from the minimal set of its unsteerable two-mode marginal CMs.

Mathematical supplement

To ensure that this thesis is complete, we also include a mathematical supplement. Specifically, this appendix includes definitions of metric and normalized vector spaces, Hilbert space, operators, and working with operators, along with other terms relevant to this thesis. We will refer to some of the following definitions throughout the text. The theory was compiled with the help of notes written during the course of study and books [31, 32].

I. Vector spaces

Definition 1 (Vector space)**.** *Vector space* $\mathcal{V}$ is a set of elements (vectors) closed with respect to the operations of vector addition and multiplication of vectors by a number (scalar). Every two vectors $|u\rangle$,$|v\rangle \in \mathcal{V}$[1] and two numbers a, $b \in \mathbb{C}$ must satisfy:

1. $|u\rangle + |v\rangle = |v\rangle + |u\rangle$,
2. $|u\rangle + |0\rangle = |u\rangle$ (existence of zero vector),
3. $a(|u\rangle + |v\rangle) = a\,|v\rangle + a\,|u\rangle$,
4. $1\,|u\rangle = |u\rangle$ (existence of identity element of scalar multiplication),
5. $(a + b)\,|u\rangle = a\,|u\rangle + b\,|u\rangle$,
6. $a(b\,|u\rangle) = (ab)\,|u\rangle$,
7. $0\,|u\rangle = 0$ (existence of zero element of scalar multiplication).

Definition 2 (Linear independence)**.** A set of vectors $|u_1\rangle$, $|u_2\rangle$, ...,$|u_N\rangle \in \mathcal{V}$ is said to be *linearly independent*, if there exists scalars c_1, c_2, ..., $c_N \in \mathbb{C}$, such that the linear combination of the vectors $\sum_{i=1}^{N} c_i\,|u_i\rangle = 0$ if and only if $c_1 = c_2 = ... = c_N = 0$.

A vector space is N-dimensional if it contains N linearly independent vectors. We shall call a vector space infinite-dimensional if for every natural number N we can find N linearly independent vectors.

Definition 3 (Ray)**.** A set of vectors $a\,|u\rangle$ with arbitrary $a \neq 0$ and fixed $|u\rangle \neq 0$ will be called a *ray*.

Definition 4 (Linear span)**.** Consider a set of vectors $S = \{|u_i\rangle\}_{i=1}^{N}$. The set of all linear combinations of vectors from S is denoted by span(S) and is called the *linear span*.

Definition 5 (Basis)**.** A set of vectors $\{|u_i\rangle\}_{i=1}^{N}$, such that the vectors are linearly independent and their span$(S) = \mathcal{V}$, is called a *basis*.

[1] The notation of vectors $|u\rangle$,$|v\rangle$ is called bra-ket notation or Dirac notation, $|u\rangle$ is called ket-vector and $|u\rangle^{\dagger} = \langle u|$ is called bra-vector.

II. Metric space

Definition 6 (Metric space)**.** *Metric space* is an ordered pair $(M,\ \rho)$ where M is a set and ρ is a metric on M. A *metric* is a mapping $\rho : M \times M \to \mathbb{R}_0^+$ that has the following properties $\forall\, |x\rangle\,, |y\rangle\,, |z\rangle \in M$:

1. $\rho(|x\rangle\,, |y\rangle) \geq 0$, $\rho(|x\rangle\,, |y\rangle) = 0$ if and only if $|x\rangle = |y\rangle$,
2. $\rho(|x\rangle\,, |y\rangle) = \rho(|y\rangle\,, |x\rangle)$,
3. $\rho(|x\rangle\,, |y\rangle) + \rho(|y\rangle\,, |z\rangle) \geq \rho(|x\rangle\,, |z\rangle)$ (triangle inequality).

Definition 7 (Convergence in metric spaces)**.** Consider a metric space $(M,\ \rho)$ and a sequence of vectors $\{|u_n\rangle\}_{n\in\mathbb{N}}$. We say that the sequence $|u_n\rangle$ *converges* to $|u\rangle$ for $n \to \infty$, if

$$\lim_{n\to\infty} \rho(|u_n\rangle\,, |u\rangle) = 0.$$

III. Normed linear space

Definition 8 (Normed linear space)**.** *Normed linear space* or simply normed space is an ordered pair $(\mathcal{V},\ \|\cdot\|)$ where $\mathcal{V}$ is a vector space and $\|\cdot\|$ is a norm. A *norm* is a mapping $\|\cdot\| : \mathcal{V} \to \mathbb{R}_0^+$ that has the following properties $\forall\, |x\rangle\,, |y\rangle \in \mathcal{V}$:

1. $\||x\rangle\| \geq 0$, $\||x\rangle\| = 0$ if and only if $|x\rangle = 0$,
2. $\|a\,|x\rangle\| = |a| \cdot \||x\rangle\|$ $\forall a \in \mathbb{C}$,
3. $\||x\rangle + |y\rangle\| \leq \||x\rangle\| + \||y\rangle\|$.

A norm induces a metric, such that $\rho(|x\rangle\,, |y\rangle) = \||x\rangle - |y\rangle\|$. This implies that a norm preserves the properties of a metric.

Definition 9 (Generalized triangle inequality)**.** $\forall\, |x\rangle\,, |y\rangle \in \mathcal{V}$ it holds that

$$\||x\rangle - |y\rangle\| \geq |\ \||x\rangle\| - \||y\rangle\|\ |.$$

Definition 10 (Convergence in normed spaces)**.** Consider a normed vector space $(\mathcal{V},\ \|\cdot\|)$ and a sequence of vectors $\{|x_n\rangle\}_{n\in\mathbb{N}}$. We say that the sequence $|x_n\rangle$ *converges* to $|x\rangle$ for $n \to \infty$, if

$$\lim_{n\to\infty} \||x_n\rangle\| - \||x\rangle\| = 0.$$

Definition 11 (Cauchy sequence)**.** A sequence $\{|x_n\rangle\}_{n\in\mathbb{N}}$ is said to be *Cauchy sequence* if

$$\forall \epsilon > 0\ \exists\, n_0 \in \mathbb{N} \text{ such that } \forall m, n > n_0\ \ \||x_n\rangle - |x_m\rangle\| < \epsilon.$$

Every convergent sequence is a Cauchy sequence. The opposite statement is true only in finite-dimensional spaces. A space in which every Cauchy sequence is convergent is called *complete*. A complete normed vector space is called a *Banach space*.

Definition 12 (Scalar (inner) product)**.** *Scalar product* is a mapping $\langle\cdot|\cdot\rangle : \mathcal{V} \times \mathcal{V} \to \mathbb{C}$ that has the following properties $\forall x,\ y,\ z \in \mathcal{V}$:

1. $\langle x|y\rangle^* = \langle y|x\rangle$ (for complex vector space, for real vector space $\langle x|y\rangle = \langle y|x\rangle$)[2]
2. $\langle x|ay\rangle = a\,\langle x|y\rangle \;\forall a \in \mathbb{C}$,
3. $\langle x+y|z\rangle = \langle x|z\rangle + \langle y|z\rangle$,
4. $\langle x|x\rangle > 0, \langle x|x\rangle = 0$ if and only if $|x\rangle = 0$.

Properties of the scalar product include:

1. $\||x\rangle\| = \sqrt{\langle x|x\rangle}$,
2. two vectors are orthogonal if $\langle u|v\rangle = 0$,

Definition 13 (Cauchy-Schwarz inequality)**.** $\forall x,y \in \mathcal{V}$

$$|\,\langle x|y\rangle\,| \leq \sqrt{\langle x|x\rangle}\sqrt{\langle y|y\rangle} = \||x\rangle\| \cdot \||y\rangle\|.$$

A complete normed linear space (Banach space) with a scalar product is called a *Hilbert space*.

IV. Hilbert space

Definition 14 (Separable Hilbert space)**.** A Hilbert space $\mathscr{H}$ in which there exists an orthonormal basis consisting of countably many vectors is called *separable*.

Let $\mathscr{H}$ be the Hilbert space and $\{|\psi_i\rangle\}$ its base. Then any vector $|u\rangle$ can be written as

$$|u\rangle = \sum_i c_i\,|\psi_i\rangle\,,$$

where $c_i = \langle\psi_i|u\rangle$, $c_i \in \mathbb{C}$.

Definition 15 (Linear manifold)**.** A set of vectors $\mathfrak{U}$ is called a *linear manifold* if any linear combination of a (finite number of) vectors of $\mathfrak{U}$ is again an element of $\mathfrak{U}$. If the linear manifold is complete, we refer to it as a subspace.

Definition 16 (Dense linear manifold)**.** A linear manifold $\mathfrak{U}$ is *dense* in space $\mathscr{H}$ if for each vector $|\psi\rangle \in \mathscr{H}$ there exists a sequence of vectors $\{|\phi_n\rangle \in \mathfrak{U}\}$ such that

$$\lim_{n\to\infty} |\phi_n\rangle = |\psi\rangle\,.$$

V. Operators

Definition 17 (Operator)**.** *An operator* is a mapping $\hat{A} : \mathcal{V} \to \mathcal{V}$ that assigns every $|\psi\rangle$ to some $|\psi'\rangle$, i.e. $|\psi\rangle \to |\psi'\rangle$. We write $|\psi'\rangle = \hat{A}\,|\psi\rangle$. An operator has a *domain* $\mathcal{D}(\hat{A})$ and a *range* $\mathcal{R}(\hat{A})$.

In the following we will only discuss operators on the Hilbert space $\mathscr{H}$.

[2]The star $*$ denotes a complex conjugate.

Definition 18 (Addition and multiplication of operators)**.** Operator $\hat{C}$ will be called the *sum* of operators $\hat{A}$ and $\hat{B}$ $\hat{C} = \hat{A} + \hat{B}$ if $\forall \left|\psi\right\rangle$

$$\hat{C}\left|\psi\right\rangle = \hat{A}\left|\psi\right\rangle + \hat{B}\left|\psi\right\rangle.$$

Similarly, we can define the *multiplication* of operators $\hat{C} = \hat{A}\hat{B}$; $\forall \left|\psi\right\rangle$

$$\hat{C}\left|\psi\right\rangle = \hat{A}\left|\psi\right\rangle + \hat{B}\left|\psi\right\rangle.$$

Specifically $\hat{A}^2 = \hat{A}\hat{A}$ and likewise, we can define higher powers.

Multiplication of operators is not commutative, i.e. $\hat{A}\hat{B} \neq \hat{B}\hat{A}$, we therefore implement the following definition.

Definition 19 (Commutator and anticommutator)**.** An operator $[\hat{A},\hat{B}] = \hat{A}\hat{B} - \hat{B}\hat{A}$ will be called *commutator* and an operator $\{\hat{A},\hat{B}\} = \hat{A}\hat{B} + \hat{B}\hat{A}$ will be called *anticommutator*. If the commutator is equal to zero, then the operators commute

The properties of the commutator include

1. $[\hat{A},\hat{B}] = -[\hat{B},\hat{A}]$,
2. $[\hat{A},\hat{B}+\hat{C}] = [\hat{A},\hat{B}] + [\hat{A},\hat{C}]$,
3. $[\hat{A},\hat{B}\hat{C}] = [\hat{A},\hat{B}]\hat{C} + \hat{B}[\hat{A},\hat{C}]$.

Definition 20 (Linear operator)**.** An operator $\hat{A}$ is *linear* if $\forall \left|\psi_1\right\rangle, \left|\psi_2\right\rangle \in \mathcal{D}(\hat{A})$, $\forall a, b \in \mathbb{C}$

$$\hat{A}(a\left|\psi_1\right\rangle + b\left|\psi_2\right\rangle) = a\hat{A}\left|\psi_1\right\rangle + b\hat{A}\left|\psi_2\right\rangle.$$

Definition 21 (Bunded operator)**.** An operator $\hat{A}$ is *bounded* if $\exists\ c \geq 0$ such that $\forall \left|\psi\right\rangle \in \mathcal{D}(\hat{A})$

$$\|\hat{A}\left|\psi\right\rangle\| \leq c\||\psi\rangle\|.$$

The infimum of the numbers c is called the *norm* of the operator $\hat{A}$ and is denoted by $\|\hat{A}\|$. In finite-dimensional spaces, every operator is bounded.

Definition 22 (Symmetric operator)**.** An operator $\hat{A}$ is *symmetric* if

$$\left\langle \psi_1 \middle| \hat{A}\psi_2 \right\rangle = \left\langle \hat{A}\psi_1 \middle| \psi_2 \right\rangle$$

$\forall \left|\psi_1\right\rangle, \left|\psi_2\right\rangle \in \mathcal{D}(\hat{A})$ dense in $\mathscr{H}$.

A bounded symmetric operator is called a *Hermitian operator*.

Definition 23 (Adjoint operator)**.** Let $\hat{A}$ be an operator with dense domain $\mathcal{D}(\hat{A})$ in $\mathscr{H}$. Then there exists an *(Hermitian) adjoint* operator $\hat{A}^\dagger$ [3] such that

$$\left\langle \psi_1 \middle| \hat{A}^\dagger\psi_2 \right\rangle = \left\langle \hat{A}\psi_1 \middle| \psi_2 \right\rangle$$

$\forall \left|\psi_1\right\rangle, \left|\psi_2\right\rangle \in \mathcal{D}(\hat{A})$. It holds that

$$\|\hat{A}\| = \|\hat{A}^\dagger\|,\ (\hat{A}^\dagger)^\dagger = \hat{A},\ (\hat{A}+\hat{B})^\dagger = \hat{A}^\dagger + \hat{B}^\dagger,\ (\hat{A}\hat{B})^\dagger = \hat{B}^\dagger\hat{A}^\dagger.$$

[3] The dagger denotes Hermitian adjoint. For matrices, the Hermitian adjoint stands for $\hat{A}^\dagger = (\hat{A}^*)^T$.

Definition 24 (Self-adjoint operator)**.** An operator $\hat{A}$ is *self-adjoint* if $\hat{A} = \hat{A}^\dagger$.

For bounded operators, the terms symmetric, Hermitian and self-adjoint are equivalent.

Definition 25 (Positive definitive operator)**.** We say that a self-adjoint operator is *positive definite* if $\forall \left|\psi\right\rangle$

$$\left\langle\psi\right| \hat{A} \left|\psi\right\rangle \geq 0.$$

Definition 26 (Inverse operator)**.** If to an operator $\hat{A}$ there exists an operator $\hat{A}^{-1}$ such that

$$\hat{A}\hat{A}^{-1} = \hat{A}^{-1}\hat{A} = \mathbb{1}$$

we call it the *inverse operator*. For inverse operators the following is true

$$(\hat{A}^{-1})^{-1} = \hat{A},\ (\hat{A}^{-1})^\dagger = (\hat{A}^\dagger)^{-1},\ (\hat{A}\hat{B})^{-1} = \hat{B}^{-1}\hat{A}^{-1}.$$

Definition 27 (Unitary operator)**.** An operator $\hat{U}$ for which holds $\mathcal{D}(\hat{U}) = \mathscr{H}$ and $\hat{U}^{-1} = \hat{U}^\dagger$ is called *unitary*.

For any unitary operator $\hat{U}$, the following holds

$$\left\langle \hat{U}\psi_1 \middle| \hat{U}\psi_2 \right\rangle = \left\langle \psi_1 | \psi_2 \right\rangle,$$

which means that the scalar product is invariant with respect to unitary transformations.

Definition 28 (Projection operator)**.** A bounded operator $\hat{P}$ satisfying $\hat{P} = \hat{P}^\dagger = \hat{P}^2$ is called a *projection operator*. If $\hat{P}_1$ is a projection operator, so is operator $\hat{P}_2 = \mathbb{1} - \hat{P}_1$, while $\hat{P}_1 + \hat{P}_2 = \mathbb{1}$ and $\hat{P}_1\hat{P}_2 = 0$.

If $\{\left|a_i\right\rangle\}_{i=1}^N$ is an orthonormal basis in $\mathscr{H}$, then the operators $\hat{P}_i = \left|a_i\right\rangle \left\langle a_i\right|$, $i =$ 1,2,...,N, are projectors onto one-dimensional subspaces spanned by vectors $\left|a_i\right\rangle$. We can write

$$\hat{P}_i \left|\psi\right\rangle = \left|a_i\right\rangle \left\langle a_i | \psi\right\rangle.$$

It holds that

$$\hat{P}_i\hat{P}_j = \begin{cases} \hat{P}_i^2 = \hat{P}_i, \text{ for } i = j, \\ \left|a_i\right\rangle \left\langle a_i | a_j\right\rangle \left\langle a_j\right| = 0, \text{ for } i \neq j, \text{ because. } \left\langle a_i | a_j\right\rangle = 0 \end{cases}$$

The projectors $\hat{P}_i$, $\hat{P}_j$ for $i \neq j$ project onto orthogonal subspaces. It further applies that

$$\sum_{i=1}^N \hat{P}_i = \sum_{i=1}^N \left|a_i\right\rangle \left\langle a_i\right| = \mathbb{1},$$

which is the so-called *completness relation*.

Definition 29 (Eigenvalues and eigenvectors)**.** Let the following hold for a non-zero vector

$$\hat{A} \left|\psi_a\right\rangle = a \left|\psi_a\right\rangle,$$

then we call a the *eigenvalue* of operator $\hat{A}$ and $\left|\psi_a\right\rangle$ the *eigenvector* corresponding to the eigenvalue of a. If there are multiple independent vectors satisfying the equation above, we say that the eigenvalue of a is *degenerate*.

The eigenvalues of a Hermitian operator are real numbers and its eigenvectors (corresponding to different eigenvalues) are orthogonal and form a basis in $\mathscr{H}$.

Definition 30 (Matrix representation of operators)**.** Let $\{|\psi_i\rangle\}$ be an orthonormal basis in $\mathscr{H}$. A Hermitian operator can be represented by a Hermitian matrix

$$\hat{A} = \mathbb{1}\hat{A}\mathbb{1} = \sum_{i,j} |\psi_i\rangle \langle\psi_i| \hat{A} |\psi_j\rangle \langle\psi_j| = \sum_{i,j} A_{ij} |\psi_i\rangle \langle\psi_j| ,$$

where $A_{ij} = \langle\psi_i| \hat{A} |\psi_j\rangle$ are matrix elements of operator $\hat{A}$ in $\{|\psi_i\rangle\}$-representation. Thus, we can write

$$\hat{A} |\psi_j\rangle = \sum_i A_{ij} |\psi_i\rangle .$$

Assume now that the eigenvectors of the operator $\hat{A}$ form a basis in $\mathscr{H}$ and let $\{|\varphi_i\rangle\}$ be that basis. Then using the equation from the Def. 29 we get

$$A_{ij} = a_i \delta_{ij},$$

where a_i are eigenvalues of operator $\hat{A}$ and δ_{ij} is Kronecker delta. Therefore, we say that an operator is expressed in its own representation by a diagonal matrix whose diagonal elements are represented by its eigenvalues. We can then write

$$\hat{A} = \sum_j a_j |\varphi_j\rangle \langle\varphi_j| = \sum_j a_j \hat{P}_j,$$

where $\hat{P}_j$ is the projection operator onto the one-dimensional subspace defined by the vector $|\varphi_j\rangle$ and the equation represents *spectral decomposition* of operator $\hat{A}$.

Definition 31 (Trace)**.** Let us consider an orthonormal basis $\{|\psi_i\rangle\}$ in $\mathscr{H}$. Then the trace of an operator $\hat{A}$ is defined as

$$\mathrm{Tr}[\hat{A}] = \sum_i \langle\psi_i| \hat{A} |\psi_i\rangle .$$

The trace has the following important properties:

1. if $\hat{A} = \hat{A}^\dagger$, then $\mathrm{Tr}[\hat{A}]$ is real,
2. $\mathrm{Tr}[a\hat{A}] = a\mathrm{Tr}[\hat{A}]$, $a \in \mathbb{C}$,
3. $\mathrm{Tr}[\hat{A} + \hat{B}] = \mathrm{Tr}[\hat{A}] + \mathrm{Tr}[\hat{B}]$,
4. $\mathrm{Tr}[\hat{A}\hat{B}] = \mathrm{Tr}[\hat{B}\hat{A}]$.

The trace of an $n \times n$ square matrix A is defined as

$$\mathrm{Tr}[A] = \sum_{i=1}^{n} a_{ii} = a_{11} + a_2 + ... + a_{nn}.$$

Definition 32 (Pauli matrices)**.** *Pauli matrices* are a set of 2x2 complex, Hermitian, unitary matrices

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

with the following properties

$$\sigma_x^2 = \sigma_y^2 = \sigma_z^2 = \mathbb{1}, \det(\sigma_i) = -1, \mathrm{Tr}[\sigma_i] = 0$$

and each has eigenvalues -1 and $+1$. Together with the unitary matrix $\mathbb{1}$, the Pauli matrices form an orthogonal basis on $\mathscr{H} = \mathbb{C}_2$.

Appendix 1

Derivation of uncertainty relation

We start with the product of the two variances

$$\langle(\Delta A)^2\rangle\langle(\Delta B)^2\rangle = \langle\psi|\,(A-\langle A\rangle)(A-\langle A\rangle)\,|\psi\rangle\,\langle\psi|\,(B-\langle B\rangle)(B-\langle B\rangle)\,|\psi\rangle\,. \quad (3.1)$$

The second expression is the multiplication of two scalar (inner) products, which means we can write it as a multiplication of two norms:

$$\langle\psi|\,(A-\langle A\rangle)(A-\langle A\rangle)\,|\psi\rangle\,\langle\psi|\,(B-\langle B\rangle)(B-\langle B\rangle)\,|\psi\rangle = \|(\Delta A)\,|\psi\rangle\|^2\|(\Delta B)\,|\psi\rangle\|^2. \quad (3.2)$$

Now we can use Cauchy-Schwarz inequality from Def. 13:

$$\|(\Delta A)\,|\psi\rangle\|^2\|(\Delta B)\,|\psi\rangle\|^2 \geq |\,\langle\psi|\,\Delta A\Delta B\,|\psi\rangle\,|^2, \quad (3.3)$$

where

$$\Delta A\Delta B = \frac{1}{2}(\Delta A\Delta B-\Delta B\Delta A+\Delta A\Delta B+\Delta B\Delta A) = \frac{1}{2}([\Delta A,\Delta B]+\{\Delta A,\Delta B\}), \quad (3.4)$$

which is equal to $\frac{1}{2}(iC+\{\Delta A,\Delta B\})$. This implies that

$$|\,\langle\psi|\,\Delta A\Delta B\,|\psi\rangle\,|^2 = \frac{1}{4}(i\,\langle\psi|\,C\,|\psi\rangle + \langle\psi|\,\{\Delta A,\Delta B\}\,|\psi\rangle\,. \quad (3.5)$$

This gives us the uncertainty relation

$$\langle(\Delta A)^2\rangle\langle(\Delta B)^2\rangle \geq \frac{1}{4}(|\langle C\rangle + |\langle\{\Delta A,\Delta B\}\rangle|)^2, \quad (3.6)$$

however, since $|\langle\{\Delta A,\Delta B\}\rangle| \geq 0$, we can write

$$\langle(\Delta A)^2\rangle\langle(\Delta B)^2\rangle \geq \frac{1}{4}|\langle C\rangle|^2. \quad (3.7)$$

Appendix 2

Concavity and convexity

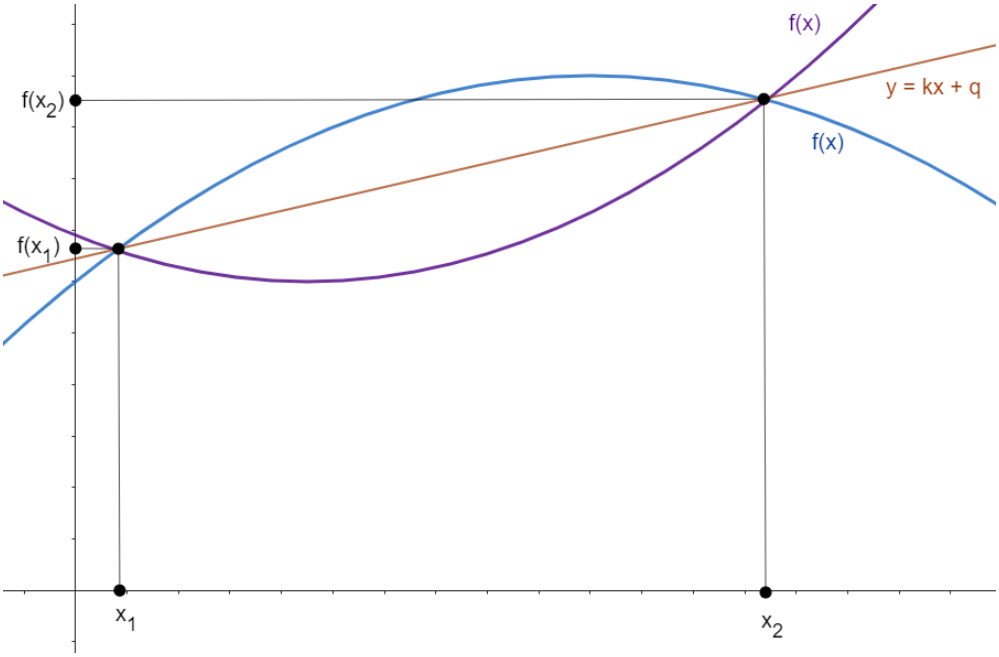

Figure 3.1: Graph of a concave and convex function. Purple function is convex and blue function is concave.

The function is convex on interval $[x_1, x_2]$ if for any $p \in [x_1, x_2]$ and $x_1 \neq x_2$

$$f(px_1 + (1-p)x_2) \leq f(x_1) + (1-p)f(x_2), \tag{3.8}$$

and the function is concave on interval $[x_1, x_2]$ if for any $p \in [x_1, x_2]$ and $x_1 \neq x_2$

$$f(px_1 + (1-p)x_2) \geq f(x_1) + (1-p)f(x_2). \tag{3.9}$$

Concavity of variance. Variance of mixture of states is mixture of the variances of those states. Mathematically:

$$\langle (\Delta A)^2 \rangle_{\sum_i p_i \rho^{(i)}} \geq \sum_i p_i \langle (\Delta A)^2 \rangle_{\rho^{(i)}}. \tag{3.10}$$

Proof.

$$\langle (\Delta A)^2 \rangle_{\sum_i p_i \rho^{(i)}} = \langle A^2 \rangle_{\sum_i p_i \rho^{(i)}} - \langle A \rangle^2_{\sum_i p_i \rho^{(i)}} = \sum_i p_i \langle A^2 \rangle_{\rho_i} - (\sum_i p_i \langle A \rangle^2_{\rho_i})^2 =$$

We can add $0 = -\sum_i p_i \langle A \rangle_{\rho_i}^2 + \sum_i p_i \langle A \rangle_{\rho_i}^2$.

$$= \sum_i p_i \langle A^2 \rangle_{\rho_i} - (\sum_i p_i \langle A \rangle_{\rho_i}^2)^2 - \sum_i p_i \langle A \rangle_{\rho_i}^2 + \sum_i p_i \langle A \rangle_{\rho_i}^2 =$$

Combining the first and third terms gives us the first term in the next equation.

$$= \sum_i p_i \langle (\Delta A)^2 \rangle_{\rho^{(i)}} + \sum_i p_i \langle A \rangle_{\rho_i}^2 - (\sum_i p_i \langle A \rangle_{\rho_i}^2)^2 \geq (*)$$

We have to prove that $\sum_i p_i \langle A \rangle_{\rho_i}^2 - (\sum_i p_i \langle A \rangle_{\rho_i}^2)^2 \geq 0$. We can add $\sum_j p_j = 1$:

$$\frac{1}{2}(\sum_j p_j \sum_i p_i \langle A \rangle_{\rho_i}^2 - 2 \sum_i p_i \langle A \rangle_{\rho_i} \sum_j p_j \langle A \rangle_{\rho_j} + \sum_i p_i \sum_j p_j \langle A \rangle_{\rho_j}^2) =$$

$$= \frac{1}{2} \sum_{i,j} p_i p_j (\langle A \rangle_{\rho_i}^2 - 2 \langle A \rangle_{\rho_i} \langle A \rangle_{\rho_j} + \langle A \rangle_{\rho_j}^2 = \frac{1}{2} \sum_{i,j} p_i p_j (\langle A \rangle_{\rho_i} + \langle A \rangle_{\rho_j})^2 \geq 0.$$

This means that

$$(*) \geq \sum_i p_i \langle (\Delta A)^2 \rangle_{\rho^{(i)}},$$

which proves concavity of variance. □

Appendix 3

The original unrounded matrix is

$$\gamma_{num}^{original} = \begin{pmatrix} 4.86812 & 0 & 10.7584 & 0 & -16.6549 & 0 \\ 0 & 6.58222 & 0 & -11.5541 & 0 & -5.59959 \\ 10.7584 & 0 & 28.1417 & 0 & -45.4207 & 0 \\ 0 & -11.5541 & 0 & 23.4418 & 0 & 11.7653 \\ -16.6549 & 0 & -45.4207 & 0 & 74.1426 & 0 \\ 0 & -5.59959 & 0 & 11.7653 & 0 & 5.96321 \end{pmatrix}. \tag{3.11}$$

Appendix 4

We will at least partially discuss how we can derive the final covariance matrix from the scheme in Fig. 2.23. The individual inputs (modes), i.e. squeeze-vacuum states, are described by matrices S_i determined by the corresponding squeeze parameter r_i

$$S_1 = \begin{pmatrix} e^{2r_1} & 0 \\ 0 & e^{-2r_1} \end{pmatrix}, S_2 = \begin{pmatrix} e^{-2r_2} & 0 \\ 0 & e^{2r_2} \end{pmatrix}, S_3 = \begin{pmatrix} e^{-2r_3} & 0 \\ 0 & e^{2r_3} \end{pmatrix}. \tag{3.12}$$

That in which exponent is the minus sign is determined by the shape of the squeezed-vacuum state, i.e. in which quadrature the state is squeezed. If we look at the Fig. 2.4, we can see that the state squeezed in p will be described by a matrix of the form S_1 and the state squeezed in x will be described by a matrix of the form S_2 and S_3. The matrices S_i of all three modes can be written into single matrix

$$S = S_1 \oplus S_2 \oplus S_3 = \begin{pmatrix} e^{2r_1} & 0 & 0 & 0 & 0 & 0 \\ 0 & e^{-2r_1} & 0 & 0 & 0 & 0 \\ 0 & 0 & e^{-2r_2} & 0 & 0 & 0 \\ 0 & 0 & 0 & e^{2r_2} & 0 & 0 \\ 0 & 0 & 0 & 0 & e^{-2r_3} & 0 \\ 0 & 0 & 0 & 0 & 0 & e^{2r_3} \end{pmatrix}. \tag{3.13}$$

Beam splitters (BS) are described by matrices determined by the trasmissivities T_{ij} and they always describe an interaction of two modes i, j (therefore the two columns of the remaining mode always contain only 0 and 1)

$$\begin{aligned} BS_1 &= \begin{pmatrix} T_{12} & 0 & \sqrt{1-T_{12}^2} & 0 & 0 & 0 \\ 0 & T_{12} & 0 & \sqrt{1-T_{12}^2} & 0 & 0 \\ -\sqrt{1-T_{12}^2} & 0 & T_{12} & 0 & 0 & 0 \\ 0 & -\sqrt{1-T_{12}^2} & 0 & T_{12} & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \\ BS_2 &= \begin{pmatrix} T_{13} & 0 & 0 & 0 & \sqrt{1-T_{13}^2} & 0 \\ 0 & T_{13} & 0 & 0 & 0 & \sqrt{1-T_{13}^2} \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ -\sqrt{1-T_{13}^2} & 0 & 0 & 0 & T_{13} & 0 \\ 0 & -\sqrt{1-T_{13}^2} & 0 & 0 & 0 & T_{13} \end{pmatrix}. \end{aligned} \tag{3.14}$$

The final covariance matrix is of the form $\gamma_3 = BS_2 \cdot BS_1 \cdot S \cdot BS_1^T \cdot BS_2^T$.

Bibliography

[1] Einstein, A., Podolsky, B., and Rosen, N. (1935). *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?* Physical Review, 47(10), 777–780. https://doi.org/10.1103/physrev.47.777

[2] Schrödinger, E. (1935). *Discussion of Probability Relations between Separated Systems.* Mathematical Proceedings of the Cambridge Philosophical Society, 31(4), 555–563. https://doi.org/10.1017/s0305004100013554

[3] Werner, R. F. (1989). *Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model.* Physical Review, 40(8), 4277–4281. https://doi.org/10.1103/physreva.40.4277

[4] Wiseman, H. M., Jones, S. B., and Doherty, A. C. (2007). *Steering, Entanglement, Nonlocality, and the Einstein-Podolsky-Rosen Paradox.* Physical Review Letters, 98(14). https://doi.org/10.1103/physrevlett.98.140402

[5] Jones, S. B., Wiseman, H. M., and Doherty, A. C. (2007). *Entanglement, Einstein-Podolsky-Rosen correlations, Bell nonlocality, and steering.* Physical Review A, 76(5). https://doi.org/10.1103/physreva.76.052116

[6] Ou, Z. Y., Pereira, S. A., Kimble, H. J., and Peng, K. C. (1992). *Realization of the Einstein-Podolsky-Rosen paradox for continuous variables.* Physical Review Letters, 68(25), 3663–3666. https://doi.org/10.1103/physrevlett.68.3663

[7] Wagner, K. E., Janousek, J., Delaubert, V., Zou, H., Harb, C. C., Treps, N., Morizur, J., Lam, P. K., and Bachor, H. (2008). *Entangling the Spatial Properties of Laser Beams.* Science, 321(5888), 541–543. https://doi.org/10.1126/science.1159663

[8] Händchen, V., Eberle, T., Steinlechner, S., Samblowski, A., Franz, T., Werner, R., and Schnabel, R. (2012). *Observation of one-way Einstein–Podolsky–Rosen steering.* Nature Photonics, 6(9), 596–599. https://doi.org/10.1038/nphoton.2012.202

[9] Wittmann, B., Ramelow, S., Steinlechner, F., Langford, N. K., Brunner, N., Wiseman, H. M., Ursin, R., and Zeilinger, A. (2012). *Loophole-free Einstein–Podolsky–Rosen experiment via quantum steering.* New Journal of Physics, 14(5), 053030. https://doi.org/10.1088/1367-2630/14/5/053030

[10] Wollmann, S., Uola, R., and Costa, A. C. (2020). *Experimental Demonstration of Robust Quantum Steering.* Physical Review Letters, 125(2). https://doi.org/10.1103/physrevlett.125.020404

[11] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., and Peev, M. (2009). *The security of practical quantum key distribution.* Reviews of Modern Physics, 81(3), 1301–1350. https://doi.org/10.1103/revmodphys.81.1301

[12] Branciard, C., Cavalcanti, E. G., Walborn, S. P., Scarani, V., and Wiseman, H. M. (2012). *One-sided device-independent quantum key distribution: Security, feasibility, and the connection with steering.* Physical Review A, 85(1). https://doi.org/10.1103/physreva.85.010301

[13] Piani, M., and Watrous, J. (2015). *Necessary and Sufficient Quantum Information Characterization of Einstein-Podolsky-Rosen Steering.* Physical Review Letters, 114(6). https://doi.org/10.1103/physrevlett.114.060404

[14] Cavalcanti, E. G., Jones, S. B., Wiseman, H. M., and Reid, M. M. (2009). *Experimental criteria for steering and the Einstein-Podolsky-Rosen paradox.* Physical Review A, 80(3). https://doi.org/10.1103/physreva.80.032112

[15] Teh, R. Y., and Reid, M. M. (2014). *Criteria for genuineN-partite continuous-variable entanglement and Einstein-Podolsky-Rosen steering.* Physical Review A, 90(6). https://doi.org/10.1103/physreva.90.062337

[16] Teh, R. Y., Gessner, M., Reid, M. D., and Fadel, M. (2022). *Full multipartite steering inseparability, genuine multipartite steering, and monogamy for continuous-variable systems.* Physical Review, 105(1). https://doi.org/10.1103/physreva.105.012202

[17] Shankar, R. (1994b). Principles of Quantum Mechanics. Plenum Publishing Corporation. Available from: http://home.ustc.edu.cn/ eclipse/Repository/

[18] Klíma, J., and Velický, B. (2016). Kvantová mechanika I. Charles University in Prague, Karolinum Press.

[19] McHugh, D., Bužek, V., and Ziman, M. (2006). *When non-Gaussian states are Gaussian: Generalization of nonseparability criterion for continuous variables.* Physical Review A, 74(5). https://doi.org/10.1103/physreva.74.050306

[20] Wigner, E. P. (1932). *On the Quantum Correction For Thermodynamic Equilibrium.* Physical Review, 40(5), 749–759. https://doi.org/10.1103/physrev.40.749

[21] Simon, R. (2000). *Peres-Horodecki Separability Criterion for Continuous Variable Systems.* Physical Review Letters, 84(12), 2726–2729. https://doi.org/10.1103/physrevlett.84.2726

[22] Frigerio, M., Destri, C., Olivares, S., and Paris, M. G. A. (2022). *Quantum steering with Gaussian states: A tutorial.* Physics Letters, 430, 127954. https://doi.org/10.1016/j.physleta.2022.127954

[23] Uola, R., Costa, A. C., Nguyen, H. T., and Gühne, O. (2019). *Quantum steering.* Reviews of Modern Physics, 92(1). https://doi.org/10.1103/revmodphys.92.015001

[24] Paraschiv, M., Miklin, N., Moroder, T., and Gühne, O. (2018). *Proving genuine multiparticle entanglement from separable nearest-neighbor marginals.* Physical Review, 98(6). https://doi.org/10.1103/physreva.98.062102

[25] Nordgren, V., Leskovjanová, O., Provazník, J., Johnston, A., Korolkova, N., and Mišta, L. (2022). *Certifying emergent genuine multipartite entanglement with a partially blind witness.* Physical Review, 106(6). https://doi.org/10.1103/physreva.106.062410

[26] Hyllus, P., and Eisert, J. (2006). Optimal entanglement witnesses for continuous-variable systems. New Journal of Physics, 8(4), 51. https://doi.org/10.1088/1367-2630/8/4/051

[27] Note Sur Une Méthode de Résolution des équations Normales Provenant de L'Application de la MéThode des Moindres Carrés a un Système D'équations Linéaires en Nombre Inférieur a Celui des Inconnues. — Application de la Méthode a la Résolution D'un Système Defini D'éQuations LinéAires. (1924). Bulletin Géodésique, 2(1), 67–77. https://doi.org/10.1007/bf03031308

[28] Tóth, G., and Petz, D. (2013). *Extremal properties of the variance and the quantum Fisher information.* Physical Review A, 87(3). https://doi.org/10.1103/physreva.87.032324

[29] Anderson, R. L. (1953). *Recent Advances in Finding Best Operating Conditions.* Journal of the American Statistical Association, 48(264), 789–798. https://doi.org/10.2307/2281072

[30] Zabinsky, Z. B. (2010). *Random Search Algorithms.* Wiley Encyclopedia of Operations Research and Management Science. https://doi.org/10.1002/9780470400531.eorms0704

[31] Kopáček, J., and Fakulta, U. K. M. (2015). *Matematická analýza nejen pro fyziky (II).*

[32] Formánek, J. (1983). *Úvod do kvantové teorie.* Academia.