Quantum Information Theory with Gaussian Systems

Von der Fakultät für Physik und Geowissenschaften
der Technischen Universität Carolo-Wilhelmina
zu Braunschweig
zur Erlangung des Grades eines
Doktors der Naturwissenschaften
(Dr. rer. nat.)
genehmigte
D i s s e r t a t i o n

von Ole Krüger
aus Braunschweig

1. Referent Prof. Dr. Reinhard F. Werner
2. Referent Prof. Dr. Martin B. Plenio
eingereicht am 5. Januar 2006
mündliche Prüfung (Disputation) am 6. April 2006
Druck 2006

Vorveröffentlichungen der Dissertation

Teilergebnisse aus dieser Arbeit wurden mit Genehmigung der Fakultät für Physik und Geowissenschaften, vertreten durch den Mentor der Arbeit, in folgenden Beiträgen vorab veröffentlicht:

Publikationen

N. Cerf, O. Krüger, P. Navez, R. F. Werner und M. M. Wolf, »Non-Gaussian Cloning of Quantum Coherent States is Optimal«, Phys. Rev. Lett. **95**, 070501 (2005).

O. Krüger und R. F. Werner, »Gaussian Quantum Cellular Automata«, in *Quantum Information with continuous variables of atoms and light*, herausgegeben von N. Cerf, G. Leuchs und E. S. Polzik (Imperial College Press, London/UK, im Druck).

Tagungsbeiträge

J. I. Cirac, G. Giedke, O. Krüger, R. F. Werner und M. M. Wolf, »Entanglement of Formation for Gaussian States with 1×1 modes«, Third Conference of ESF-QIT »Advances in quantum information processing: from theory to experiment« (Poster, Erice/Italien, 15. – 22. 3. 2003).

O. Krüger, R. F. Werner und M. M. Wolf, »Cloning Gaussian States«, DPG-Frühjahrstagung 2004 (Vortrag, München, 22. – 26. 3. 2004).

O. Krüger und R. F. Werner, »Gaussian Quantum Cellular Automata«, CVQIP'04 Workshop (Poster, Veilbronn, 2. – 5. 4. 2004).

O. Krüger und R. F. Werner, »Gaussian Quantum Cellular Automata«, EIN04 »International Symposium on Entanglement, Information & Noise« (Poster, Krzyżowa/Polen, 14. – 20. 6. 2004).

O. Krüger und R. F. Werner, »Gaussian Quantum Cellular Automata«, DPG-Frühjahrstagung 2005 (Vortrag, Berlin, 4. – 9. 3. 2005).

O. Krüger und R. F. Werner, »Gaussian Quantum Cellular Automata«, IQING 4 (Vortrag, Paris/Frankreich, 23. – 25. 7. 2005).

Contents

Quantum Cellular Automata

Private Quantum Channels

List of Figures

List of Theorems

Summary

This thesis applies ideas and concepts from quantum information theory to systems of continuous-variables such as the quantum harmonic oscillator. In particular, it is concerned with Gaussian states and Gaussian systems, which transform Gaussian states into Gaussian states. While continuous-variable systems in general require an infinite-dimensional Hilbert space, Gaussian states can be described by a finite set of parameters. This reduces the complexity of many problems, which would otherwise be hardly tractable. Moreover, Gaussian states and systems play an important role in today's experiments with continuous-variable systems, e.g. in quantum optics. Examples of Gaussian states are coherent, thermal and squeezed states of a light field mode. The methods utilized in this thesis are based on an abstract characterization of Gaussian states, the results thus do not depend on the particular physical carriers of information.

The focus of this thesis is on three topics: the cloning of coherent states, Gaussian quantum cellular automata and Gaussian private channels. Correspondingly, the main part of the thesis is divided into three chapters each of which presents the results for one topic:

3 Cloning An unknown quantum state can in general not be duplicated perfectly. This impossibility is a direct consequence of the linear structure of quantum mechanics and enables quantum key distribution. The approximate copying or »cloning« of quantum states is possible, though, and raises questions about optimal cloning. Bounds on the fidelity of cloned states provide restrictions and benchmarks for other tasks of quantum information: In quantum key distribution, bounds on cloning fidelities allow to estimate the maximum information an eavesdropper can get from intercepting quantum states in relation to noise detected by the receiver. Beyond that, any communication task which aims at the complete transmission of quantum states has to beat the respective cloning limits, because otherwise large amounts of information either remain at the sender or are dissipated into the environment.

Cloning was investigated both for finite-dimensional and for continuous-variable systems. However, results for the latter were restricted to covariant Gaussian operations. This chapter presents a general optimization of cloning operations for coherent input states with respect to fidelity. The optimal cloners are shown to be covariant with respect to translations of the input states in phase space. In contrast to the finite-dimensional case, optimization of the joint output state and of weighted combinations of individual clones yields different cloners: while the former is Gaussian, the latter is *not*. The optimal fidelities are calculated analytically for the joint case and numerically for the individual judging of two clones. For classical cloning, the opti-

mum is reached by a measurement and preparation of coherent states. The bound on classical cloning is turned into a criterion for the successful transmission of a coherent state by quantum teleportation.

4 Quantum Cellular Automata Quantum cellular automata (QCAs) are a model for universal quantum computation in translationally invariant lattice systems with localized dynamics. They provide an alternative concept for experimental realization of quantum computing as they do not require individual addressing of their constituent systems but rather rely on global parameters for the dynamics. Quantum cellular automata seem to be particularly fitted for implementation in optical lattices as well as for the simulation of lattice systems from statistical mechanics. For this purpose the QCA should be able to reproduce the ground state of a different dynamics, preferably by driving an initial state into a suitable stationary state in the limit of large time.

This chapter investigates abstract Gaussian QCAs with respect to irreversibility. As a basis, it provides methods to deal with translationally invariant systems on infinite lattices with localization conditions. A simple example of a reversible Gaussian QCA (a nonsqueezing dynamics with nearest-neighbor interaction on the infinite linear chain of harmonic oscillators) proves that even reversible QCAs show aspects of irreversibility. In addition, we characterize the stationary states for this type of dynamics. While reversible QCAs exhibit properties which make their characterization particularly convenient both for finite-dimensional and Gaussian continuous-variable systems, the definition of irreversible QCAs causes problems. Gaussian systems provide a testbed to illuminate these difficulties. We present different concepts of localization and their impact on the requirements in the definition of QCAs.

5 Private Quantum Channels Besides the generation of classical keys for encryption, quantum cryptography provides a scheme to encrypt quantum information by a one-time pad with classical key. The elements of the key are in one-to-one correspondence with the elements of a finite set of unitary encryption operations. A sequence of input states is encrypted by applying the operations as determined by the sequence of key elements. A receiver with the same key sequence can easily decipher these states by applying the respective inverse unitary operations. However, to an eavesdropper without knowledge about the key sequence, the output state of the encryption looks like a random mixture of all encryption operations applied to the input and weighted with the probability of the key elements. For a suitable set of encryption operations, this output does not contain any information about the input state. Hence any eavesdropping must remain unsuccessful and the encrypted state can be safely sent over a public quantum channel. The encryption thus establishes a private quantum channel for sender and receiver with the same key.

We construct a private quantum channel for the sequential encryption of coherent states with a classical key, where the key elements have finite precision. This scheme can be made arbitrarily secure, i.e. the trace norm distance of any two encrypted states is bounded from above. The necessary precision of the key elements depends

on the desired security level, an energy constraint for the input states and a maximal length of correlations over the sequence of input states. For the case of independent one-mode input states, we explicitly estimate this precision, i.e. the number of key bits needed per input state, in terms of these parameters.

1 Introduction

As quantum systems can behave radically different from classical systems, the concept of information based on quantum mechanics opens up new possibilities for the manipulation, storage and transmission of information. Quantum information theory [1] explores these possibilities and transforms them into applications such as quantum computation and quantum cryptography. For suitable problems, these concepts can perform better than their classical counterparts. A prominent example is the Shor algorithm [2], which factorizes integers efficiently on a quantum computer; it is thus exponentially faster than the known classical algorithms.

Quantum information is encoded in the state of a quantum system. To obtain results which are independent of a physical realization, quantum information theory usually refers to the physical carriers of information only by an abstract description based on quantum mechanics. The basic unit of quantum information is the qubit, which in analogy to a classical bit is modeled as a generic two-level quantum system.

Fundamental features of quantum mechanics are linearity and the tensor product structure of the Hilbert space formalism, which allow for coherent superpositions of quantum states and entanglement, i.e. correlations which are stronger than classically[1] possible. Hence in contrast to a classical bit, a qubit can take on not only logical values »0« and »1«, corresponding to the ground state and excited state, but also any coherent superposition. While such effects enable an exponential speedup in quantum computation, some tasks pose difficulties. In particular, it is impossible to perfectly duplicate a quantum state. However, an approximate copying or »cloning« can be achieved, where the quality of the clones is strictly limited. This implies that quantum information cannot be completely transformed into classical information, because otherwise the classical information could be used to generate multiple copies of the respective quantum state. However, quantum teleportation can transmit quantum information by sending only classical information if in addition sender and receiver share entangled states, which are used to restore the quantum states from the classical data.

For the processing of quantum information, finite-dimensional systems, i.e. qubits and generalizations to d-level systems, are perfectly suited. Moreover, they can be implemented in a large variety of physical systems, without a leading contender so far. The transmission of quantum information over large macroscopic distances, however, is usually implemented by means of an optical scheme. In principle, single photons can be used to carry qubits in their polarization degree of freedom. Unfortunately, single photons are fragile objects which have to be treated with care and tend to get lost. As an alternative, the information can be encoded into a mode of the

1 Read: in a local realistic model.

electromagnetic field of »bright«[2] laser beams. A field mode is described as a quantum harmonic oscillator with field operators Q, P corresponding to the quadrature components of the complex amplitude. Since Q and P have continuous eigenvalue spectrum, the mode is a continuous-variable system, which cannot be represented on a finite-dimensional Hilbert space.[3]

Gaussian continuous-variable states are characterized by a Gaussian Wigner quasi-probability function. They naturally arise as the ground and thermal states of quadratic bosonic Hamiltonians, in particular for the standard harmonic oscillator,

$$H = \tfrac{1}{2}\left(Q^2 + P^2\right).$$

(Throughout this thesis, we set $\hbar = 1$. Similarly, we do not distinguish different modes by their frequency but always assume $m, \omega = 1$. Units of physical quantities are chosen accordingly.) Hence Gaussian states are relevant wherever quantum systems are described by such Hamiltonians. Examples of Gaussian states in quantum optics include coherent states (pure states with minimal uncertainty, »displaced vacuum«), thermal states (coherent states with additional classical Gaussian noise) and squeezed states (with reduced variance for Q or P). In particular, the output states of lasers are approximated by coherent states.

Gaussian states are also mathematically appealing, because they can be described by a finite number of parameters for each mode. The underlying phase space related to the canonical commutation relation,

$$[Q, P] = \mathrm{i}\,\mathbb{1}\,,$$

provides a rich mathematical structure. This makes Gaussian states much easier to handle than general continuous-variable states, which require tools for infinite-dimensional Hilbert spaces: Restricting questions to Gaussian states allows to investigate problems which would otherwise be hardly tractable. Moreover, Gaussian states are extremal among all states with the same first and second moments with respect to certain functionals: It is a standard result of statistical mechanics that Gaussian states maximize the von Neumann entropy $S(\rho) = -\operatorname{tr}[\rho \log \rho]$ for fixed energy. Only recently, Wolf et al. [3] have proved that a similar result holds for a more general class of functionals, which comprises important examples from quantum information theory (entanglement measures, key distillation rates, channel capacities). One can thus assume an unknown quantum state to be Gaussian in order to obtain reliable bounds on such quantities. For these reasons, Gaussian states are of particular relevance for the study of continuous-variable systems.

While quantum information theory for finite-dimensional systems is quite far developed, continuous-variable systems have not yet attracted equal attention. In this

2 This emphasizes the contrast to very weak laser pulses with approximately 0.1 photons per pulse, which are used to emulate single-photon sources.

3 Consider e.g. position and momentum operators Q and P, which obey the canonical commutation relation $[Q, P] = \mathrm{i}\,\mathbb{1}$. If Q and P could be described by finite-dimensional matrices, the trace of the commutator would vanish, $\operatorname{tr}[Q\,P - P\,Q] = \operatorname{tr}[Q\,P] - \operatorname{tr}[P\,Q] = \operatorname{tr}[Q\,P] - \operatorname{tr}[Q\,P] = 0$. This contradicts $\operatorname{tr}[\mathbb{1}] = \dim \mathcal{H}$.

thesis, three well-established concepts of quantum information theory are transfered to the continuous-variable Gaussian world: the cloning of coherent states (chapter 3), Gaussian quantum cellular automata (chapter 4) and Gaussian private quantum channels (chapter 5). In addition, chapter 2 provides the common ground for all chapters with an overview of the basic tools of phase space as well as Gaussian states and systems. The main chapters can be read independently of each other and provide a selfcontained introduction to the respective topics.

2 Basics of Gaussian systems

This chapter provides basic tools and notions for the handling of continuous-variable systems in general and for Gaussian systems in particular. It does not strive to extensively introduce this field but rather tries to provide common prerequisites for the rest of this thesis in a concise way. For a more thorough treatment of the matter see the forthcoming review [5] on quantum information with Gaussian systems and the book by Holevo [6] for topics regarding phase space and Gaussian states. Fundamental aspects from functional analysis are covered in [7]. For various other topics the reader is referred to the references mentioned below. The following sections deal, in this order, with the general concepts of phase space for continuous-variable quantum systems, Gaussian states and Gaussian quantum channels.

Throughout this chapter, we implicitly refer to a preview version of [5]; a supplementary source was [d].

Remark on notation: We denote the adjoint of an operator A with respect to a scalar product by a star, i.e. as A^*. Complex conjugation of scalars or matrices is indicated by a bar, e.g. as $\overline{\alpha}$ or $\overline{A}$. For simplicity, we generally set $\hbar = 1$; units of physical quantities are understood to be chosen accordingly. The identity operator and the identity matrix are denoted by the symbol $\mathbb{1}$. In some instances, the dimension of matrices is specified by a single index, e.g. $\mathbb{1}_f$.

2.1 Phase space

As in classical mechanics (cf. e.g. [4]), a system of f degrees of freedom (or modes) can be described in a *phase space* (Ξ, σ), which consists of a real vector space Ξ of dimension $2f$ equipped with a *symplectic form* $\sigma\colon \Xi \times \Xi \to \mathbb{R}$. This antisymmetric bilinear form gives rise to a *symplectic scalar product* $\sigma(\xi, \eta) = \sum_{k=1}^{2f} \xi_k^{\mathrm{T}} \cdot \sigma_{k,l} \cdot \eta_l$ implemented by the *symplectic matrix* $\sigma_{k,l} = \sigma(e_k, e_l)$, where $\{e_k\}$ is an orthonormal basis in Ξ. We will only deal with cases where σ is nondegenerate, i.e. if $\sigma(\xi, \eta) = 0$ for all $\xi \in \Xi$, then $\eta = 0$. To keep notation simple, we will not distinguish between bilinear forms and their implementing matrices in a particular basis. For translationally invariant systems, we will also identify any matrix γ of entries $\gamma_{x,y}$ with the function $\gamma(x - y) = \gamma_{x,y}$ yielding these entries. Similarly, we will refer to the linear space Ξ alone as the phase space if the symplectic form is of secondary importance in a particular context.

We introduce the *symplectic adjoint* A^+ of a matrix A with respect to the symplectic scalar product by

$$\sigma(A\,\xi, \eta) = \sigma(\xi, A^+ \eta)\,. \tag{2.1}$$

Since $\sigma(A\,\xi,\eta) = (A\,\xi)^{\mathrm{T}} \cdot \sigma \cdot \eta$, the symplectic transpose is explicitly obtained as $A^{+} = \sigma^{-1} \cdot A^{\mathrm{T}} \cdot \sigma$.

The symplectic form governs the abstract description of a quantum system via the canonical commutation relations (CCR) between canonical or field operators R_k for $k = 1, 2, \ldots, 2f$:

$$[R_k, R_l] = \mathrm{i}\sigma_{k,l}\,\mathbb{1}\,. \tag{2.2}$$

For a system of f harmonic oscillators, the field operators correspond to position and momentum operators Q_j and P_j of each mode $j = 1, 2, \ldots, f$. In quantum optics Q and P are replaced by the quadrature components of the electromagnetic field. By fixing a particular harmonic oscillator as a reference for Q, P of each mode and choosing a *modewise* ordering of the field operators,

$$R_{2j-1} = Q_j\,, \quad R_{2j} = P_j\,,$$

the symplectic matrix takes on a standard form:

$$\sigma = \bigoplus_{j=1}^{f} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \mathbb{1}_f \otimes \sigma_0 \quad \text{for} \quad \sigma_0 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \tag{2.3}$$

(where $\mathbb{1}_f$ indicates the $f \times f$ identity matrix). In a different ordering, where all position operators are grouped together and followed by all momentum operators, i.e.

$$R_j = Q_j\,, \quad R_{f+j} = P_j\,,$$

the symplectic matrix has a different block structure:

$$\sigma = \begin{pmatrix} 0 & \mathbb{1}_f \\ -\mathbb{1}_f & 0 \end{pmatrix}. \tag{2.4}$$

We refer to this ordering as *blockwise* or (Q,P)-block ordering. Depending on the situation, one form for σ or the other might be advantageous. In either case, the set of field operators can be compactly written as a vector $\vec{R} = (Q_1, P_1, Q_2, P_2, \ldots, Q_f, P_f)$ or $\vec{R} = (Q_1, Q_2, \ldots, Q_f, P_1, P_2, \ldots, P_f)$.

An equivalent description of a continuous-variable quantum system does not use the field operators Q and P, but builds upon the annihilation and creation operators a_k and a_k^*, respectively, which are defined by

$$a_k = (Q_k + \mathrm{i}P_k)/\sqrt{2}$$

and because of (2.2), (2.3) obey the bosonic commutation relations

$$[a_k, a_l^*] = \delta_{k,l}\,\mathbb{1}\,, \quad [a_k, a_l] = [a_k^*, a_l^*] = 0\,.$$

The operator

$$\hat{N}_k = a_k^*\,a_k = (Q_k^2 + P_k^2 - \mathbb{1})/2$$

yields as its expectation value the occupation number of mode k, i.e. the number of quanta in this mode.

The commutation relation (2.2) requires that the Hilbert space for any representation of the R_k is of infinite dimension and that the R_k are not bounded. In quantum mechanics, the usual representation of the CCR for each degree of freedom is the Schrödinger representation on the Hilbert space $\mathcal{H} = \mathcal{L}^2(\mathbb{R}, \mathrm{d}x)$ of square-integrable functions, where Q and $\mathrm{i}P$ act by multiplication and differentiation with respect to the variable x.[1] However, this representation leaves room for ambiguities, as is discussed with a counterexample in [7, Ch. VIII.5]. This problem can be overcome by building the theory upon suitable exponentials of the field operators instead. A possible choice is to use the family of bounded, unitary Weyl operators

$$\mathrm{W}_\xi = \mathrm{e}^{\mathrm{i}\xi^{\mathrm{T}}\cdot\sigma\cdot\vec{R}} \quad \text{for } \xi \in \Xi\,; \text{ in particular } \mathrm{W}_0 = \mathbb{1}\,. \tag{2.5}$$

Hence for σ in standard form and $\xi = (q_1, p_1, \ldots, q_f, p_f)$, the Weyl operators can be written explicitly as

$$\mathrm{W}_\xi = \exp\bigl(\mathrm{i}\textstyle\sum_{k=1}^{f}(q_k\,P_k - p_k\,Q_k)\bigr)\,. \tag{2.6}$$

By the CCR (2.2), the Weyl operators satisfy the Weyl relations

$$\mathrm{W}_\xi\ \mathrm{W}_\eta = \mathrm{e}^{-\mathrm{i}\sigma(\xi,\eta)/2}\ \mathrm{W}_{\xi+\eta} \quad \text{and} \tag{2.7a}$$

$$\mathrm{W}_\xi\ \mathrm{W}_\eta = \mathrm{e}^{-\mathrm{i}\sigma(\xi,\eta)}\ \mathrm{W}_\eta\ \mathrm{W}_\xi\ . \tag{2.7b}$$

Note that by these relations and unitarity of W_ξ, the inverse of a Weyl operator is

$$\mathrm{W}_\xi^* = \mathrm{W}_{-\xi}\ .$$

Remark on notation: Where appropriate, we expand the argument of Weyl operators, i.e. we write equivalently to each other

$$\mathrm{W}_\xi \equiv \mathrm{W}_{\xi_1,\xi_2,\ldots,\xi_n} \equiv \mathrm{W}_{q_1,p_1,\ldots,q_n,p_n}\ .$$

It is implicitly understood that $\xi = (\xi_1, \xi_2, \ldots, \xi_n)$ and $\xi_i = (q_i, p_i)$. Occasionally, we find it convenient to write the argument of Weyl operators in parentheses instead as an index:

$$\mathrm{W}(\xi) \equiv \mathrm{W}_\xi\ .$$

In reverse, the generators R_k of a family of unitary operators which satisfy the relations (2.7) give rise to the CCR (2.2), cf. [7, Ch. VIII.5]. Moreover, for representations of the Weyl relations in a finite-dimensional phase space, the Stone-von Neumann theorem states conditions for unitary equivalence [5, 7]:

1 That is, for $\psi \in \mathcal{L}^2(\mathbb{R}, \mathrm{d}x)$: $Q\,\psi(x) = x\,\psi(x)$ and $\mathrm{i}P\,\psi(x) = \frac{\mathrm{d}}{\mathrm{d}x}\,\psi(x)$.

Theorem 2.1 (Stone, von Neumann):
Two families $\mathrm{W}^{(1)}$ and $\mathrm{W}^{(2)}$ of unitary operators satisfying the Weyl relations (2.7) over a finite-dimensional phase space which are

(i) strongly continuous, i.e. $\forall\psi\in\mathcal{H}\colon\ \lim_{\psi\to 0}\left\|\psi-\mathrm{W}_\xi^{(i)}\,\psi\right\|=0$, and

(ii) irreducible, i.e. $\Big(\forall\xi\in\Xi\colon\ \big[\mathrm{W}_\xi^{(i)},A\big]=0\Big)\implies A\propto\mathbb{1}$,

are unitarily equivalent, i.e. there exists a unitary operator U mapping one system to the other by $\mathrm{W}_\xi^{(1)}=U^*\,\mathrm{W}_\xi^{(2)}\,U$.

Note that the statement of this theorem is definitely not true for an infinite-dimensional phase space. We will only consider Weyl systems which are strongly continuous and irreducible. For finitely many degrees of freedom, these systems are thus equivalent to the Schrödinger representation, where the Weyl operator of a single mode acts on the Hilbert space $\mathcal{H}=\mathcal{L}^2(\mathbb{R},\mathrm{d}x)$ of square-integrable functions by

$$\mathrm{W}_{q,p}\ \psi(x)=\mathrm{e}^{\mathrm{i}(qP-pQ)}\,\psi(x)=\mathrm{e}^{-\mathrm{i}qp/2-\mathrm{i}px}\,\psi(x+q)\,.$$

Note that by this definition the Weyl operators act on the field operators as a shift by $-\xi$, i.e.

$$\mathrm{W}_\xi^*\,R_k\,\mathrm{W}_\xi=R_k-\xi_k\,\mathbb{1}\,. \tag{2.8}$$

Since by (2.7b) and (2.3) Weyl operators of different modes commute, they can be decomposed into a tensor product of Weyl operators on single modes

$$\mathrm{W}_{\xi_1,\xi_2,\ldots,\xi_f}=\bigotimes_{j=1}^{f}\mathrm{W}_{\xi_j}\,, \tag{2.9}$$

where the Weyl operators on different phase spaces are distinguished only by the dimension of their argument. The unitary equivalence to the Schrödinger representation can thus be established for each mode separately. Note that by this decomposition Weyl operators act on each mode locally.

As the Weyl relations (2.7) give rise to the CCR (2.2), the family of Weyl operators is a sufficient basis to describe a continuous-variable system for a given phase space (Ξ,σ). In order to gain more structure, the Weyl operators are used to constitute an algebra whose norm closure is the CCR algebra $\mathrm{ccr}(\Xi,\sigma)$ of the phase space. This provides powerful algebraic tools for the description of continuous-variable quantum systems. Since by (2.9) the Weyl operators can be decomposed into tensor factors representing single modes, the CCR algebra can be represented by bounded operators on a tensor product of representation Hilbert spaces for single modes, i.e. by $\mathcal{B}(\mathcal{H}^{\otimes f})$ for systems with f degrees of freedom.

Irreducible representations of the Weyl operators allow for a convenient result, namely that operators which commute with all Weyl operators are multiples of the identity:

Lemma 2.2:
Let $X \in \mathrm{ccr}(\Xi, \sigma)$. If for all phase space vectors $\eta \in \Xi$

$$\mathrm{W}_\eta \, X \, \mathrm{W}_\eta^* = \mathrm{e}^{\mathrm{i}\sigma(\xi,\eta)} \, X, \text{ then } X = \lambda \, \mathrm{W}_\xi \,, \text{ where } \lambda \in \mathbb{C} \,.$$

Proof: Consider $X' = X \, \mathrm{W}_\xi^*$ and assume that $\mathrm{W}_\eta \, X \, \mathrm{W}_\eta^* = \mathrm{e}^{\mathrm{i}\sigma(\xi,\eta)} \, X$ for all $\eta \in \Xi$. Then

$$\mathrm{W}_\eta \, X' \, \mathrm{W}_\eta^* = \mathrm{e}^{-\mathrm{i}\sigma(\xi,\eta)} \; \mathrm{W}_\eta \, X \, \mathrm{W}_\eta^* \, \mathrm{W}_\xi^* = X \, \mathrm{W}_\xi^* = X' \,.$$

Since the Weyl representation is supposed to be irreducible, $X' = \lambda \, \mathbb{1}$ follows (cf. the statement of Theorem 2.1). □

2.1.1 Noncommutative Fourier transform and characteristic functions

The Weyl operators implement a noncommutative Fourier transform and thus an equivalence between suitable operators and complex functions on phase space. This equivalence allows to transform questions on quantum systems from operator algebras to complex analysis. A trace class operator[2] ρ and a complex, Lebesgue integrable phase space function $\chi(\xi)$ are related to each other by the Weyl transform and its inverse,

$$\rho = (2\pi)^{-f} \int_\Xi \mathrm{d}^{2f}\xi \; \chi_\rho(\xi) \, \mathrm{W}_\xi^* \,, \tag{2.10a}$$

$$\chi(\xi) = \mathrm{tr}[\rho \, \mathrm{W}_\xi], \tag{2.10b}$$

where the integral is over a phase space Ξ of dimension $2f$ and ρ acts on a corresponding Hilbert space $\mathcal{H}$. The pair of ρ and χ_ρ constitute a quantum Fourier transform by a noncommutative version of the Parseval relation connecting scalar products of operators with those of functions [5]:

Theorem 2.3 (Parseval relation):
Let Ξ be a phase space for f degrees of freedom. Consider a strongly continuous, irreducible family of Weyl operators which are represented on a Hilbert space $\mathcal{H}$. Then the mapping $\rho \mapsto \chi(\xi) = \mathrm{tr}[\rho \, \mathrm{W}_\xi]$ is an isometry from the Hilbert-Schmidt operators[3] on $\mathcal{H}$ to the function space $\mathcal{L}^2(\Xi, (2\pi)^{-f} \, \mathrm{d}^{2f}\xi)$. Hence the scalar products equal each other,

$$\mathrm{tr}[\rho_1^* \, \rho_2] = (2\pi)^{-f} \int_\Xi \mathrm{d}^{2f}\xi \; \overline{\chi_1(\xi)} \, \chi_2(\xi) \,. \tag{2.11}$$

2 A bounded operator $A \in \mathcal{B}(\mathcal{H})$ belongs to the trace class $\mathcal{T}_1(\mathcal{H})$ if $\mathrm{tr}\big[|A|\big] = \mathrm{tr}\big[(A^*A)^{1/2}\big] < \infty$.

3 The mapping is defined on trace class operators $\mathcal{T}_1(\mathcal{H})$ and extends to Hilbert-Schmidt operators $\mathcal{T}_2(\mathcal{H})$, i.e. bounded operators $A \in \mathcal{B}(\mathcal{H})$ with $\mathrm{tr}[A^*A] < \infty$. The class $\mathcal{T}_2(\mathcal{H})$ is a Hilbert space with scalar product $(\rho_1, \rho_2) = \mathrm{tr}[\rho_1^* \, \rho_2]$.

For a proof of this theorem, see e.g. [6]. An extended discussion of Fourier transforms between operators and functions can be found in [8]. A useful application of the Parseval relation (2.11) is the computation of the overlap $|\langle\psi|\phi\rangle|^2$ between pure states $|\psi\rangle$ and $|\phi\rangle$:

$$\big|\langle\psi|\phi\rangle\big|^2 = \mathrm{tr}\big[|\psi\rangle\langle\psi|\,|\phi\rangle\langle\phi|\big] = (2\pi)^{-f}\int_\Xi \mathrm{d}^{2f}\xi\,\overline{\chi_\psi(\xi)}\,\chi_\phi(\xi)\,,$$

where χ_ψ and χ_ϕ denote the characteristic functions of the two states.

The relations (2.10) connect properties of the density operator ρ with those of the characteristic function χ_ρ:

- ▷ Boundedness: $\big|\chi_\rho(\xi)\big| \leq \|\rho\|_1$.
- ▷ Normalization: $\mathrm{tr}[\rho] = \mathrm{tr}[\rho\,\mathrm{W}_0] = 1 \iff \chi_\rho(0) = 1$.
- ▷ Purity: $\chi_\rho(\xi)$ corresponds to a pure state[4] if and only if $\rho^2 = \rho$ or $\mathrm{tr}[\rho^2] = 1$ and hence if
$$\int_\Xi \mathrm{d}^{2f}\xi\,\big|\chi_\rho(\xi)\big|^2 = (2\pi)^f. \tag{2.12}$$
- ▷ Symmetry: Since ρ is hermitian, $\chi_\rho(\xi) = \overline{\chi_\rho(-\xi)}$.
- ▷ Continuity: $\chi(\xi)$ is continuous if and only if it corresponds to a normal state, i.e. to a state which can be described by a density matrix.

A given function $\chi(\xi)$ is the characteristic function of a quantum state if and only if it obeys a quantum version of the Bochner-Khinchin criterion [6]: $\chi(\xi)$ has to be normalized to $\chi(0) = 1$, continuous at $\xi = 0$ and σ-positive definite, i.e. for any number $n \in \mathbb{N}$ of phase space vectors $\xi_1, \xi_2, \ldots, \xi_n \in \Xi$ and coefficients $c_1, c_2, \ldots, c_n \in \mathbb{C}$ it has to fulfill

$$\sum_{k,l=1}^{n} c_k\,\overline{c_l}\,\chi(\xi_k - \xi_l)\,\exp\big(\mathrm{i}\sigma(\xi_k,\xi_l)/2\big) \geq 0\,. \tag{2.13}$$

The characteristic function in (2.10b) can be taken as the *classical* Fourier transform of a function. With this interpretation, the result of a classical inverse Fourier

4 A density matrix ρ corresponds to a pure state if and only if $\rho^2 = \rho$, i.e. if ρ is a projector; due to the normalization $\mathrm{tr}[\rho] = 1$, this projector is of rank one, $\rho = |\psi\rangle\langle\psi|$. If the state is not pure, it is mixed and can be written as a convex combination of pure states $|\psi_i\rangle\langle\psi_i|$:

$$\rho = \textstyle\sum_i \lambda_i\,|\psi_i\rangle\langle\psi_i|,\ \text{where } \lambda_i \geq 0 \text{ and } \sum_i \lambda_i = 1\,.$$

For continuous-variable states, this convex combination might be continuous, i.e. an integral over a classical probability density $\lambda(z)$:

$$\rho = \int \mathrm{d}z\ \lambda(z)\,|\psi_z\rangle\langle\psi_z|,\ \text{where } \lambda(z) \geq 0 \text{ and } \int \mathrm{d}z\ \lambda(z) = 1\,.$$

transform of $\chi_\rho(\xi)$ with respect to the variable $\sigma\cdot\eta$ is the Wigner function [9] $\mathcal{W}_\rho(\eta)$ of ρ,

$$\mathcal{W}_\rho(\xi) = (2\pi)^{-2f}\int_\Xi \mathrm{d}\eta\, \mathrm{e}^{\mathrm{i}\xi^{\mathrm{T}}\cdot\sigma\cdot\eta}\,\chi_\rho(\eta)\,. \tag{2.14}$$

The Wigner function is related to expectation values of the parity operator $\mathbb{P}$ [10]. For more than one mode, $\mathbb{P}$ is a tensor product of single-mode parity operators, which act on the respective field operators by inversion of sign. Hence $\mathbb{P}\,R_k\,\mathbb{P} = -R_k$. Moreover, it is unitary and hermitian, $\mathbb{P}^{-1} = \mathbb{P}^* = \mathbb{P}$. With this,

$$\mathcal{W}_\rho(\xi) = \pi^{-f}\ \mathrm{tr}\big[\rho\ \mathrm{W}_\xi\,\mathbb{P}\,\mathrm{W}_\xi^*\big]\,. \tag{2.15}$$

The description of a quantum state by the Wigner function as a quasi-probability distribution on phase space is equivalent to the characteristic function.[5] However, we mostly use the characteristic function $\chi(\xi)$ to describe states.

Similar to classical probability theory, the derivatives of the characteristic function of a state yield the *moments* with respect to the field operators [6]. In particular, the first and second moments are derived in terms of modified field operators $\vec{R}' = \sigma\cdot\vec{R}$ as

$$\begin{aligned}\frac{1}{\mathrm{i}}\,\frac{\partial}{\partial\xi_k}\,\chi_\rho(\xi)\Big|_{\xi=0} &= \mathrm{tr}\big[\rho\,R'_k\big]\,,\\ -\frac{\partial^2}{\partial\xi_k\,\partial\xi_l}\,\chi_\rho(\xi)\Big|_{\xi=0} &= \tfrac{1}{2}\,\mathrm{tr}\big[\rho\,\{R'_k,R'_l\}_+\big]\,,\end{aligned}$$

where $\{R'_k,R'_l\}_+ = R'_kR'_l + R'_lR'_k$ denotes the anti-commutator of R'_k and R'_l. From these moments we define the *displacement vector* d' by

$$d'_k = \mathrm{tr}\big[\rho\,R'_k\big] \tag{2.16}$$

and the *covariance matrix* γ' by

$$\gamma'_{k,l} = \mathrm{tr}\Big[\rho\,\big\{\big(R'_k-\langle R'_k\rangle\big),\big(R'_l-\langle R'_l\rangle\big)\big\}_+\Big] = \mathrm{tr}\big[\rho\,\{R'_k,R'_l\}_+\big] - 2\langle R'_k\rangle\langle R'_l\rangle\,, \tag{2.17}$$

where the prime indicates quantities with respect to the modified field operators. Using the commutation relation (2.2), this is equivalent to

$$\mathrm{tr}\Big[\rho\,\big(R'_k-\langle R'_k\rangle\big)\big(R'_l-\langle R'_l\rangle\big)\Big] = \tfrac{1}{2}\gamma'_{k,l} + \tfrac{i}{2}\sigma_{k,l}\,. \tag{2.18}$$

Note that necessarily $\gamma+\mathrm{i}\sigma\geq 0$: Consider the matrix

$$A_{k,l} = \mathrm{tr}\big[\rho\,\big(R_k-\langle R_k\rangle\big)\big(R_l-\langle R_l\rangle\big)\big] = (\gamma+\mathrm{i}\sigma)/2$$

5 Note that there exist other quasi-probability functions, namely the P- and the Q-function, which give rise to other characteristic functions. These correspond to different orderings of the field operators.

for complex vectors $\xi \in \mathbb{C}^{2f}$ together with the operator $L = \sum_{k=1}^{2f} \xi_k R_k$. Then A is positive-semidefinite due to $\langle\xi|A|\xi\rangle = \mathrm{tr}[\rho L^* L] \geq 0$. Since γ is real, this is equivalent to $\gamma - \mathrm{i}\sigma \geq 0$. Moreover, as σ is antisymmetric, the inequality implies $\gamma \geq 0$.

Due to the symplectic scalar product $\xi^{\mathrm{T}} \cdot \sigma \cdot \vec{R}$ in the definition (2.5) of the Weyl operators, these relations are written in terms of modified field operators $\vec{R}' = \sigma \cdot \vec{R}$. In the standard basis of (2.3), this transformation is local to each mode,

$$\begin{pmatrix} Q'_j \\ P'_j \end{pmatrix} = \sigma_0 \cdot \begin{pmatrix} Q_j \\ P_j \end{pmatrix}.$$

Since we are usually not concerned with specific physical realizations but rather with qualitative results for all continuous-variable systems, we mostly drop the distinction between R'_k and R_k. Note, however, the effect of displacing a state ρ with Weyl operators, $\rho' = \mathrm{W}_\eta \, \rho \, \mathrm{W}_\eta^*$, on the characteristic function:

$$\chi'_\rho(\xi) = \mathrm{tr}[\mathrm{W}_\eta \, \rho \, \mathrm{W}_\eta^* \; \mathrm{W}_\xi] = \mathrm{tr}[\rho \; \mathrm{W}_\eta^* \, \mathrm{W}_\eta \, \mathrm{W}_\xi] = \chi_\rho(\xi) \, \mathrm{e}^{-\mathrm{i}\xi^{\mathrm{T}} \cdot \sigma \cdot \eta} \,. \tag{2.19}$$

In field operators R'_k, the state is displaced by the vector $-\sigma \cdot \eta$, which corresponds to a translation by $-\eta$ in R_k; cf. also Eq. (2.8).

2.1.2 Symplectic transformations

While an orthogonal transformation leaves the scalar product over a (real) vector space unchanged, a real symplectic or canonical transformation S preserves the symplectic scalar product of a phase space,

$$\sigma(S\,\xi, S\,\eta) = \sigma(\xi, \eta) \text{ for all } \xi, \eta \in \Xi \,.$$

By this definition, a symplectic transformation for f degrees of freedom is a real $2f \times 2f$ matrix such that $S^{\mathrm{T}} \cdot \sigma \cdot S = \sigma$. The group of these transformations is the real *symplectic group*, denoted as $\mathrm{Sp}(2f, \mathbb{R})$. Moreover, with $S \in \mathrm{Sp}(2f, \mathbb{R})$ also $S^{\mathrm{T}}, S^{-1}, -S \in \mathrm{Sp}(2f, \mathbb{R})$, where the inverse of S is given by $S^{-1} = \sigma \, S^{\mathrm{T}} \, \sigma^{-1}$. Symplectic transformations have determinant $\det S = +1$. In addition, the symplectic matrix σ itself is a symplectic transformation, as can be seen from one of its standard forms (2.3) or (2.4). The inverse is $\sigma^{-1} = \sigma^{\mathrm{T}} = -\sigma$. For the special case of a single mode, the symplectic group consist of all real $2{\times}2$ matrices with determinant one, i.e. $\mathrm{Sp}(2, \mathbb{R}) = \mathrm{SL}(2, \mathbb{R})$. Extensive discussions of the symplectic group, including the topics of this section, can be found e.g. in [11, 12, 13].

By (2.2), symplectic transformations of the vector of field operators, $\vec{R}' = S\,\vec{R}$, do not change the canonical commutation relations; they do not alter the physics of a continuous-variable system but merely present a change of the symplectic basis. Since σ is itself a symplectic transformation, this argument justifies neglecting the distinction between R'_k and R_k in the computation of the moments above. Under a symplectic transformation S, displacement vector and covariance matrix are modified according to $d \mapsto S{\cdot}d$ and $\gamma \mapsto S^{\mathrm{T}}{\cdot}\gamma{\cdot}S$. Weyl operators are mapped to Weyl operators

by a linear transformation of the argument, $\mathrm{W}_\xi \mapsto \mathrm{W}_{S\,\xi}$. By Theorem 2.1, the two families of Weyl operators are connected by a unitary transformation U_S such that

$$\mathrm{W}_{S\,\xi} = U_S^*\,\mathrm{W}_\xi\,U_S\,.$$

The operators U_S form the so-called *metaplectic representation* of the symplectic group $\mathrm{Sp}(2f,\mathbb{R})$.[6]

Every symplectic transformation S can be decomposed in several ways of which we only consider the Euler decomposition into diagonal squeezing transformations and symplectic orthogonal transformations:

Theorem 2.4:
Every symplectic transformation $S \in \mathrm{Sp}(2f,\mathbb{R})$ can be decomposed as (written in standard ordering of $\vec{R}$)

$$S = K \cdot \left(\bigoplus_{j=1}^{f} \begin{pmatrix} \mathrm{e}^{r_j} & 0 \\ 0 & \mathrm{e}^{-r_j} \end{pmatrix} \right) \cdot K'\,, \tag{2.20}$$

where $K, K' \in \mathrm{Sp}(2f,\mathbb{R}) \cap \mathrm{SO}(2f)$ are symplectic and orthogonal and $r_j \in \mathbb{R}$ are called squeezing parameters.

Remark: This implies that $\mathrm{Sp}(2f,\mathbb{R})$ is not compact. In fact, $\mathrm{Sp}(2f,\mathbb{R}) \cap \mathrm{SO}(2f)$ is the maximal compact subgroup of $\mathrm{Sp}(2f,\mathbb{R})$.

Similar to real-valued normal matrices, which can be diagonalized by orthogonal transformations, symmetric positive matrices can be diagonalized by symplectic transformations. This corresponds to a decomposition into *normal modes*, i.e. into modes which decouple from each other:

Theorem 2.5 (Williamson):
Any symmetric positive $2f \times 2f$ matrix A can be diagonalized by a symplectic transformation $S \in \mathrm{Sp}(2f,\mathbb{R})$ such that

$$S A S^{\mathrm{T}} = \bigoplus_{j=1}^{f} a_j\,\mathbb{1}_2\,,$$

where $a_j > 0$. The *symplectic eigenvalues* a_j of A can be obtained as the (usual) eigenvalues of $\mathrm{i}\sigma A$, which has spectrum $\mathrm{spec}(\mathrm{i}\sigma A) = \{\pm a_j\}$.

6 Due to an ambiguity in a complex phase, the operators U_S form a faithful representation of the metaplectic group $\mathrm{Mp}(2f,\mathbb{R})$, which is a two-fold covering of the $\mathrm{Sp}(2f,\mathbb{R})$.

2.2 Gaussian states

Gaussian quantum states are states of continuous-variable systems which have a Gaussian characteristic function[7], i.e. $\chi(\xi)$ has the shape of a classical Gaussian distribution. By convention, we write a Gaussian $\chi(\xi)$ as

$$\chi(\xi) = \mathrm{e}^{-\xi^{\mathrm{T}}\cdot\gamma\cdot\xi/4+\mathrm{i}\xi^{\mathrm{T}}\cdot d}\,, \tag{2.21}$$

where d and γ are the real-valued *displacement vector* and the real-valued, symmetric, positive-semidefinite *covariance matrix* from (2.16) and (2.17), respectively. (Note that the remark on modified field operators applies.) The characteristic function and thus the Gaussian state is solely determined by γ and d.

For a given Gaussian function $\chi(\xi)$ to be the characteristic function of a (Gaussian) state, it has to obey the Bochner-Khinchin criterion (see above). Due to its shape (2.21), one readily has $\chi(0) = 1$ and continuity at $\xi = 0$. The requirement of σ-positive definiteness (2.13) translates into the *state condition* on the covariance matrix γ:

$$\gamma + \mathrm{i}\sigma \geq 0\,. \tag{2.22}$$

Since γ is real, this is equivalent to $\gamma - \mathrm{i}\sigma \geq 0$. Moreover, as σ is antisymmetric, the condition implies $\gamma \geq 0$. That the state condition is necessary for γ to be the covariance matrix of a state has been shown above. Sufficiency follows from (2.21) and (2.13), see [6]. Hence any real, symmetric, positive matrix γ which complies with the state condition describes a valid Gaussian quantum state.[8]

The inequality (2.22) expresses uncertainty relations for the field operators. In particular, for a diagonal matrix γ with entries $\gamma_1, \gamma_1, \gamma_2, \gamma_2, \ldots, \gamma_{2f}, \gamma_{2f}$, the inequality requires that the eigenvalues $\gamma_j \pm 1$ of $\gamma + \mathrm{i}\sigma$ be positive and thus that $\gamma_j \geq 1$. By the definition of the covariance matrix in (2.17), this imposes Heisenberg's uncertainty relation

$$\left(\langle Q_j^2\rangle - \langle Q_j\rangle^2\right)\left(\langle P_j^2\rangle - \langle P_j\rangle^2\right) \geq \tfrac{1}{4}\,. \tag{2.23}$$

Since due to Theorem 2.5 any covariance matrix can be diagonalized by a symplectic transformation, the above argument is valid even in the general case, where the diagonal entries are replaced by the symplectic eigenvalues.

If for the covariance matrix γ of a single mode the inequality (2.22) is »sharp«, i.e. $\gamma + \mathrm{i}\sigma$ has one eigenvalue zero, a Gaussian state with this covariance matrix γ has minimal uncertainty, since the single symplectic eigenvalue is $\gamma_1 = 1$. Moreover, by (2.12), such Gaussian states are pure. Since according to Theorem 2.5 the symplectic eigenvalues can be found from $\mathrm{i}\sigma\,\gamma$, the condition for purity of a Gaussian state in terms of its covariance matrix γ can be written as

$$(\sigma\,\gamma)^2 = -\mathbb{1}\,.$$

7 Equivalently, a Gaussian state is characterized by a Gaussian Wigner function.

8 While the state condition (2.22) on the covariance matrix is always necessary, it is in general not sufficient to assure σ-positive definiteness of the characteristic function for an arbitrary, non-Gaussian state.

If, in contrast, a Gaussian state ρ is not pure, its covariance matrix γ can be written as a sum $\gamma = \gamma_{\text{pure}} + \gamma_{\text{noise}}$ of a covariance matrix γ_{pure} belonging to a pure state ρ_{pure}, and a positive-semidefinite matrix γ_{noise}. While γ_{pure} is subject to the state condition, γ_{noise} is *not* restricted by (2.22). The decomposition of γ results in a decomposition of the characteristic function of ρ, which can be written as a product

$$\chi(\xi) = \chi_{\text{pure}}(\xi)\, \exp\bigl(-\xi^{\mathrm{T}} \cdot \gamma_{\text{noise}} \cdot \xi/4\bigr)\,, \tag{2.24}$$

where $\chi_{\text{pure}}(\xi)$ is the characteristic function of ρ_{pure}. Transforming $\chi(\xi)$ back into a density operator by (2.10a) in this form results in a convolution of ρ_{pure} with the classical Gaussian probability density with covariance matrix γ_{noise} [8]:

$$\rho = \int \mathrm{d}\xi\ \exp\bigl(-\xi^{\mathrm{T}} \cdot \sigma^{\mathrm{T}}\, \gamma_{\text{noise}}^{-1}\, \sigma \cdot \xi/4\bigr)\ \mathrm{W}_\xi\, \rho_{\text{pure}}\, \mathrm{W}_\xi^*\,. \tag{2.25}$$

(Note the change $\gamma_{\text{noise}} \mapsto \sigma^{\mathrm{T}} \cdot \gamma_{\text{noise}}^{-1} \cdot \sigma$ due to the Fourier transform.) From this relations, γ_{noise} can be interpreted as Gaussian noise which is added to the pure state ρ_{pure} in order to obtain the mixed state ρ.

2.2.1 Coherent, thermal and squeezed states

Coherent, thermal and squeezed states of the standard harmonic oscillator with Hamiltonian $H = (Q^2 + P^2)/2$ are special instances of Gaussian states which each represent particular characteristics of general Gaussian states. We introduce these states for the case of a single mode; the generalization to more modes is based on Theorem 2.5 and covered in the next section. All three types of states are characterized by their covariance matrix γ: Coherent states have $\gamma = \mathbb{1}$, thermal states have $\gamma = \tau\,\mathbb{1}$ ($\tau > 1$) and squeezed states have one of the diagonal elements of γ smaller than 1, e.g. $\gamma = \left(\begin{smallmatrix} r & 0 \\ 0 & 1/r \end{smallmatrix}\right)$.

Coherent states are pure Gaussian states with covariance matrix $\gamma = \mathbb{1}$ and arbitrary displacement vector d, i.e. they can be defined by a characteristic function of the form

$$\chi(\xi) = \mathrm{e}^{-\xi^2/4 + \mathrm{i}\xi^{\mathrm{T}} \cdot d}\,. \tag{2.26}$$

Since coherent states differ from each other only in the displacement d, they can be generated from the coherent state ρ_0 with $d = 0$ by displacing it with Weyl operators according to (2.19):

$$\rho_d = \mathrm{W}_{\sigma^{-1} \cdot d}\ \rho_0\, \mathrm{W}_{\sigma^{-1} \cdot d}^*\,,$$

where ρ_d is the coherent state with displacement d. To stress this relation, we alternatively write the characteristic function of coherent states with displacement vector $d \equiv \sigma \cdot \alpha$ as

$$\chi(\xi) = \mathrm{e}^{-\xi^2/4 - \mathrm{i}\xi^{\mathrm{T}} \cdot \sigma \cdot \alpha} \tag{2.27}$$

such that $\rho_{\sigma\cdot\alpha} = \mathrm{W}_\alpha\, \rho_0\, \mathrm{W}_\alpha^*$.

As pure states, coherent states correspond to Hilbert space vectors $|\alpha\rangle$, which we label by the phase space vector α determining the displacement in (2.26). This allows to write

$$|\alpha\rangle = \mathrm{W}_\alpha\,|0\rangle\,. \tag{2.28}$$

The state $|0\rangle\langle 0|$ has expectation value zero in the field operators and is a minimum uncertainty state (see above). Moreover, among all such states it has the smallest possible expectation value of the operator Q^2+P^2, since its variances with respect to the field operators are equal,[9] $\langle Q^2\rangle = \langle P^2\rangle = \frac{1}{2}$. Considering that $Q^2+P^2 = 2\hat{N}+\mathbb{1}$ and hence $\mathrm{tr}[\rho_0\,\hat{N}] = 0$, $|0\rangle\langle 0|$ necessarily is the vacuum state.

The relation (2.28) allows to compute the overlap between two coherent states:

$$\langle\alpha|\beta\rangle = \langle 0|\,\mathrm{W}_\alpha^*\,\mathrm{W}_\beta\,|0\rangle = \langle 0|\,\mathrm{W}_{\beta-\alpha}\,|0\rangle\,\mathrm{e}^{\mathrm{i}\sigma(\alpha,\beta)/2} = \mathrm{e}^{-(\beta-\alpha)^2/4+\mathrm{i}\sigma(\alpha,\beta)/2}\,. \tag{2.29}$$

This overlap is strictly nonzero, hence coherent states are not orthogonal to each other.

Coherent states are eigenstates of the annihilation operator $a = (Q+\mathrm{i}P)/\sqrt{2}$: denoting $\alpha = (\alpha_q,\alpha_p)$, one has[10]

$$\begin{aligned} a\,|\alpha\rangle &= \mathrm{W}_\alpha\,\mathrm{W}_\alpha^*\,a\,\mathrm{W}_\alpha\,|0\rangle \\ &= \tfrac{1}{\sqrt{2}}\,\mathrm{W}_\alpha\,\big((Q-\alpha_q\,\mathbb{1})+\mathrm{i}(P-\alpha_p\,\mathbb{1})\big)\,|0\rangle \\ &= \mathrm{W}_\alpha\,a\,|0\rangle - \tfrac{1}{\sqrt{2}}\,(\alpha_q+\mathrm{i}\alpha_p)\,\mathrm{W}_\alpha\,|0\rangle \\ &= -\tfrac{1}{\sqrt{2}}\,(\alpha_q+\mathrm{i}\alpha_p)|\alpha\rangle\,. \end{aligned} \tag{2.30}$$

The expectation value of the occupation number operator $\hat{N} = a^*a$ in a coherent state is thus $\mathrm{tr}\big[|\alpha\rangle\langle\alpha|\,\hat{N}\big] = \langle\alpha|\,a^*a\,|\alpha\rangle = |\alpha|^2/2$. This can be interpreted as the mean energy of a system in the coherent state $|\alpha\rangle\langle\alpha|$ if the result is scaled by the characteristic energy $\hbar\,\omega$ of the mode.

A thermal state of the Hamiltonian $H = (Q^2+P^2)/2$ with covariance matrix $\gamma = \tau\,\mathbb{1}$, $\tau > 1$ is by (2.24) and (2.25) a classical mixture of coherent states, where $\gamma_{\mathrm{pure}} = \mathbb{1}$ and the noise is described by $\gamma_{\mathrm{noise}} = (\tau-1)\,\mathbb{1}$:

$$\rho_\tau = \int\mathrm{d}\xi\;\exp\!\big(-\tfrac{1}{4}\,\xi^2\,(\tau-1)^{-1}\big)\;\mathrm{W}_\xi\,|\alpha\rangle\langle\alpha|\,\mathrm{W}_\xi^*\,. \tag{2.31}$$

The displacement of ρ_τ is the same as of $|\alpha\rangle\langle\alpha|$.

9 Recall that for $a,b,c\in\mathbb{R}$ and $a,b,c>0$, the quantity $a+b$ under the restriction $a\,b=c$ is minimized for $a=b$.

10 Note that this differs from the convention where coherent states are labeled by their eigenvalue with respect to the annihilation operator a:

$$a\,|\tfrac{\alpha_q+\mathrm{i}\alpha_p}{\sqrt{2}}\rangle = \tfrac{\alpha_q+\mathrm{i}\alpha_p}{\sqrt{2}}\,|\tfrac{\alpha_q+\mathrm{i}\alpha_p}{\sqrt{2}}\rangle\,.$$

Defining a complex number $\alpha = (\alpha_q+\mathrm{i}\alpha_p)/\sqrt{2}$, this reads $a\,|\alpha\rangle = \alpha\,|\alpha\rangle$. Consequentially, relations between coherent states look different, e.g. the overlap (2.29) is given by $\langle\alpha|\beta\rangle = \exp(-|\alpha|^2/2-|\beta|^2/2+\overline{\alpha}\,\beta)$.

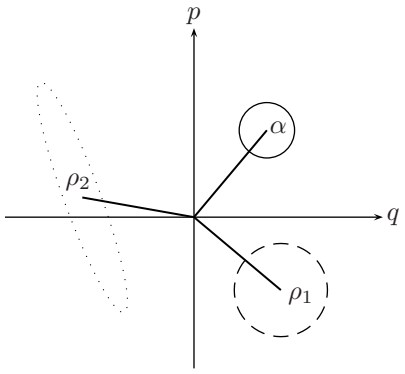


Figure 2.1:
Depicting Gaussian states in phase space by »lollipop sticks« for the single-mode case. The examples are a coherent state α, a thermal state ρ_1 and a squeezed state ρ_2. The amplitude is visualized by a vector (q, p) whose components are the expectation values of the canonical operators for the state, i.e. $q = \mathrm{tr}\big[|\alpha\rangle\langle\alpha|\, Q\big]$ and $p = \mathrm{tr}\big[|\alpha\rangle\langle\alpha|\, P\big]$. The covariance matrix is indicated by the circle or ellipse which it describes geometrically, centered at the endpoint of the respective amplitude vector. Note that the squeezed ellipse can be oriented arbitrarily with respect to the coordinate system and the vector.

In contrast to coherent and thermal states, squeezed states have one of the variances for the field operators smaller than $\frac{1}{2}$, i.e. below the limit of Heisenberg's uncertainty relation (2.23). Correspondingly, one of the diagonal elements of the covariance matrix γ is smaller than 1. However, this need not be true for any particular basis of the phase space, but can apply to rotated field operators. In the geometric interpretation of Fig. 2.1, the covariance matrix of the squeezed state ρ_2 describes an ellipse which in one direction is smaller than the circle of a coherent state. For a single-mode pure squeezed state, the covariance matrix can be written as $\gamma = S^{\mathrm{T}} \cdot \mathbb{1} \cdot S$, where S is a symplectic transformation. In the Euler decomposition (2.20) of S, the inner orthogonal transformation K' is irrelevant; hence

$$\gamma = \tau\, K^{\mathrm{T}} \cdot \begin{pmatrix} \mathrm{e}^{2r} & 0 \\ 0 & \mathrm{e}^{-2r} \end{pmatrix} \cdot K,$$

where the squeezing parameter $r \in \mathbb{R}$ deforms the circle to an ellipse and K is any orthogonal 2×2 matrix describing the rotation with respect to the basis of the phase space.

2.2.2 Spectral decomposition and exponential form

Consider a Gaussian state ρ with zero displacement or, equivalently, a symplectic basis $\vec{R}$ in which the displacement has been transformed to zero by applying suitable Weyl operators. Theorem 2.5 implies that every covariance matrix γ of the state ρ can be diagonalized by a symplectic transformation S. The corresponding

unitary operator U_S implements this transformation on a density operator ρ such that $U_S\,\rho\,U_S^*$ decomposes into a tensor product of one-mode Gaussian states:

$$\rho = \bigotimes_{j=1}^{f} \rho_j\,, \tag{2.32a}$$

where the ρ_j are thermal states with covariance matrix $\gamma_j\,\mathbb{1}$ and γ_j as the symplectic eigenvalues of γ. Computing $\langle m_j|\,\rho_j\,|n_j\rangle$ from (2.30) and (2.31) for the eigenvectors $|n_j\rangle$ of the occupation number operator $\hat{N}_j$ for mode j yields the spectral decomposition

$$\rho_j = \frac{2}{\gamma_j+1}\sum_{n_j=0}^{\infty}\left(\frac{\gamma_j-1}{\gamma_j+1}\right)^{n_j}|n_j\rangle\langle n_j|\,. \tag{2.32b}$$

The eigenvalues $\nu_{n_1,n_2,\ldots,n_f}$ of the full state ρ with f modes can be labeled by the occupation number of each of its normal modes and are given by

$$\nu_{n_1,n_2,\ldots,n_f} = \prod_{j=1}^{f}\frac{2}{\gamma_j+1}\,\left(\frac{\gamma_j-1}{\gamma_j+1}\right). \tag{2.33}$$

The occupation number expectation value N_j of a single mode (undisplaced) is obtained as

$$N_j = \mathrm{tr}\big[\rho_j\,a_j^*a_j\big] = \frac{2}{\gamma_j+1}\sum_{n_j=0}^{\infty}\left(\frac{\gamma_j-1}{\gamma_j+1}\right)^{n_j} n_j = \frac{\gamma_j-1}{2}\,.$$

Note that $N_j \geq 0$ corresponds to the condition on symplectic eigenvalues, $\gamma_j \geq 1$, induced by the state condition (2.22). If the expectation value N of the occupation number follows a Bose distribution, $N = (\mathrm{e}^{-\beta}-1)^{-1}$ with inverse temperature β, the resulting single-mode state ρ is a Gibbs state, $\rho = \mathrm{e}^{-\beta\hat{N}}/\,\mathrm{tr}[\mathrm{e}^{-\beta\hat{N}}]$.

The above spectral decomposition (2.32b) directly gives rise to an exponential form for the Gaussian state ρ_j of a single mode j [d]:

$$\rho_j = \exp\Big(\log 2 - \log(\gamma_j+1) + \big(\log(\gamma_j-1) - \log(\gamma_j+1)\big)\,a_j^*a_j\Big),$$

where a_j^* and a_j are the creation and annihilation operators, respectively, associated with this mode. Since $a_j^*\,a_j = (Q_j^2+P_j^2-\mathbb{1})/2$, the above can be recast as

$$\rho_j = \exp\Big(\tfrac{1}{2}\,\big(\log(\gamma_j-1) - \log(\gamma_j+1)\big)\,(Q_j^2+P_j^2) - \tfrac{1}{2}\,\log(\gamma_j^2-1) + \log 2\Big).$$

Generalizing this to the case of f modes and denoting the symplectic basis where

the density operator decomposes into a tensor product by a prime, we arrive at

$$\rho = \exp\left(\frac{1}{2}\sum_{k,l=1}^{2f} M'_{k,l} R'_k R'_l - \frac{1}{2}\sum_{j=1}^{f} \log(\gamma_j^2 - 1)\right), \tag{2.34a}$$

$$\text{where } M' = \bigoplus_{j=1}^{f} \big(\log(\gamma_j - 1) - \log(\gamma_j + 1)\big)\, \mathbb{1}_2\,. \tag{2.34b}$$

The exponential form for ρ is especially useful to compute entropy expressions involving $\log\rho$, e.g. $S(\rho) = -\operatorname{tr}[\rho\log\rho]$. By (2.34a), we get

$$\log\rho = \left(\frac{1}{2}\sum_{k,l=1}^{2f} M'_{k,l} R'_k R'_l - \frac{1}{2}\sum_{j=1}^{f} \log(\gamma_j^2 - 1)\right). \tag{2.35}$$

2.2.3 Entangled states

The term entanglement describes quantum correlations which are stronger than possible with any local realistic model. In a bipartite setting, these correlations pertain between two parties, conventionally named »Alice« and »Bob«, associated with Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively. A nonentangled or separable state ρ_{sep} on $\mathcal{H}_A \otimes \mathcal{H}_B$ can be interpreted as a convex combination of product states [14]:

$$\rho_{\text{sep}} = \sum_i \lambda_i\, \rho_A^i \otimes \rho_B^i\,, \quad \text{where } \lambda_i \geq 0 \text{ and } \sum_i \lambda_i = 1\,, \tag{2.36}$$

where the ρ_A^i are states on $\mathcal{H}_A$ and ρ_B^i on $\mathcal{H}_B$. A state which can be written in this form is classically correlated, since it can be reproduce by choosing states ρ_A^i and ρ_B^i for systems A and B with classical probability λ_i. Otherwise, the state is entangled. Note that for a separable pure state the decomposition in (2.36) is trivial, i.e. a pure state is either a product state or it is entangled.

In general, it is not easy to verify that a given state is separable or entangled, since a decomposition (2.36) might not be obvious to find. However, there exist several criteria to assist in this process. A necessary criterion for separability is the positivity of the partial transpose of the density operator [15, 16]. Partial transposition is a transposition with respect to only one of the tensor factors: If ρ is a density operator on $\mathcal{H}_A \otimes \mathcal{H}_B$ and Θ denotes the matrix transposition, the partial transpose of ρ with respect to system A is obtained as

$$\rho^{\mathrm{T}_A} = (\Theta \otimes \mathrm{id})(\rho)\,.$$

If ρ is PPT with respect to system A, i.e. has positive partial transpose $\rho^{\mathrm{T}_A} \geq 0$, it is also PPT with respect to B by full transposition of the inequality. Note that transposition of a matrix depends on the basis in which it is carried out. However, the eigenvalues of the partial transposition are independent of the basis.

In phase space, transposition of Hermitian density operators is the same as complex conjugation, which in turn can be identified with inversion of sign for the momenta [15], i.e. $P \mapsto -P$ while $Q \mapsto Q$ under Θ. This corresponds to a »reversal of time« or rather a reversal of time evolution. As a density operator ρ of a bipartite Gaussian state is positive if its covariance matrix obeys the state condition (2.22), $\gamma + \mathrm{i}\sigma_A \oplus \sigma_B \geq 0$ (where σ_A, σ_B are the symplectic forms for systems A and B), the partial transpose ρ^{T_A} is positive if the covariance matrix obeys

$$\gamma + \mathrm{i}(-\sigma_A) \oplus \sigma_B \geq 0\,,$$

where the sign on σ_A reflects the change of sign for momenta in the CCR (2.2).

While the PPT criterion is necessary for separability, it is sufficient only for »small« systems: $\mathbb{C}^2 \otimes \mathbb{C}^2$ and $\mathbb{C}^2 \otimes \mathbb{C}^3$ in finite dimensions [17], Gaussian states with $1\times n$ modes for continuous-variable systems [18]. In particular, the criterion fails if both parties A and B of a Gaussian states have more than one mode (an explicit example is presented in [18]). Since the entanglement of entangled states with positive partial transpose cannot be freely converted into other forms, the entanglement is »bound« and the sates are called »PPT-bound entangled«.

2.2.4 Singular states

In a general sense, a quantum state ω is a normalized positive linear functional[11] on the algebra of observables [19], i.e. here on $\mathrm{ccr}(\Xi, \sigma)$ for f degrees of freedom:

$$\omega\colon\ \mathrm{ccr}(\Xi,\sigma) \to \mathbb{C},\ \text{where } \omega(X^*X) \geq 0 \text{ for all } X \in \mathrm{ccr}(\Xi,\sigma) \text{ and } \omega(\mathbb{1}) = 1\,.$$

Note that $\mathbb{1} = \mathrm{W}_0 \in \mathrm{ccr}(\Xi, \sigma)$. A state is *normal* if it can be described by a density operator, i.e. a positive trace class operator ρ on the representation Hilbert space $\mathcal{H}^{\otimes f}$:

$$\omega(X) = \mathrm{tr}[\rho\, X]\,.$$

Otherwise, the state ω is *singular* and can be decomposed into a normal part ω_n given by a density operator and a *purely singular* contribution ω_s, which has expectation value zero for all compact operators[12]: $\omega = \omega_n + \omega_s$ (cf. Section 3.3.1). Singular states have a characteristic function by

$$\chi(\xi) = \omega\big(\mathrm{W}_\xi\big)$$

and can thus be Gaussian if $\chi(\xi)$ is a Gaussian (2.21).

If the CCR algebra is represented on the Hilbert space $\mathcal{H}^{\otimes f}$, then the normalized positive linear functionals ω on $\mathrm{ccr}(\Xi, \sigma)$ form the space $\mathcal{B}^*\big(\mathcal{H}^{\otimes f}\big)$. Similarly, the linear space generated by the density operators is denoted by $\mathcal{B}_*\big(\mathcal{H}^{\otimes f}\big)$, whose closure in the weak topology is $\mathcal{B}^*\big(\mathcal{H}^{\otimes f}\big)$.

11 Normalized positive linear functionals are automatically bounded and continuous.

12 Compact operators on a Hilbert space are those which can be approximated in norm by finite rank operators, i.e. operators represented as a *finite* sum of terms $|\phi\rangle\langle\psi|$, cf. e.g. [7, Vol. I].

2.3 Gaussian channels

Quantum channels describe transformations between quantum states which correspond to physical operations. For example, applying a unitary transformation U to a state ρ as $U\rho U^*$ is a channel and corresponds to a change of basis or a symmetry transformation. Formally, a quantum channel T_* in the Schrödinger picture is a trace-preserving, completely positive linear map on the trace class operators. For Hilbert spaces $\mathcal{H}$ and $\mathcal{K}$ of input and output systems, respectively,

$$T_*\colon \mathcal{B}_*(\mathcal{H}) \to \mathcal{B}_*(\mathcal{K}),\ \mathrm{tr}\big[T_*(\rho)\big] = \mathrm{tr}[\rho]\,.$$

T_* has to be positive, i.e. map positive trace class operators to positive trace class operators, and it has to preserve the trace to assure normalization. However, positivity alone is not enough. In addition, applying T_* to part of a quantum state has to yield an admissible quantum state for the whole system. This is assured by complete positivity: A map T_* is completely positive if $(T_* \otimes \mathrm{id})(\rho')$ is positive for every positive trace class operator ρ' on a composite Hilbert space $\mathcal{H} \otimes \mathcal{H}'$ and id is the identity on $\mathcal{H}'$.

Rather than transforming states (Schrödinger picture), a corresponding transformation can be applied to observables (Heisenberg picture), such that both yield the same expectation values. Instead of preserving the trace, this transformation is unital, i.e. it preserves $\mathbb{1}$. The Heisenberg picture variant T of a channel is thus determined by

$$\mathrm{tr}\big[\rho\, T(A)\big] = \mathrm{tr}\big[T_*(\rho)\, A\big], \quad \text{where} \quad T\colon \mathcal{B}(\mathcal{K}) \to \mathcal{B}(\mathcal{H}),\ T(\mathbb{1}) = \mathbb{1}\,. \tag{2.37}$$

For simplicity, we will also refer to input and output spaces by the respective CCR algebras, e.g. for a channel in the Heisenberg picture $T\colon\ \mathrm{ccr}(\Xi_{\mathrm{out}}, \sigma_{\mathrm{out}}) \to \mathrm{ccr}(\Xi_{\mathrm{in}}, \sigma_{\mathrm{in}})$.

Gaussian channels have been considered e.g. in [20, 21, 22, 23, 24, 53]. A channel is Gaussian if it maps Gaussian states to Gaussian states in the Schrödinger picture. In the Heisenberg picture, such channels are quasi-free, i.e. they map Weyl operators to multiples of Weyl operators. A general Gaussian channel for f degrees of freedom acts by

$$T(\mathrm{W}_\xi) = \mathrm{W}_{\Gamma\cdot\xi}\ \mathrm{e}^{-g(\xi,\xi)/4 + \mathrm{i}\xi^{\mathrm{T}}\cdot d}\,, \tag{2.38}$$

where Γ is a real $2f \times 2f$ matrix, g is a real, symmetric bilinear transformation and d is a real vector of length $2f$. The transformations Γ and g cannot be chosen arbitrary, but are subject to a restriction in order for T to be completely positive. In [20], this condition is stated and proven. For ease of reference, we repeat the theorem in our notation:

Theorem 2.6:
A unital map $T\colon\ \mathrm{ccr}(\Xi_{\mathrm{out}}, \sigma_{\mathrm{out}}) \to \mathrm{ccr}(\Xi_{\mathrm{in}}, \sigma_{\mathrm{in}})$ of the form (2.38) is completely positive if and only if

$$g + \mathrm{i}\sigma_{\mathrm{out}} - \mathrm{i}\Gamma^{\mathrm{T}}\sigma_{\mathrm{in}}\,\Gamma \geq 0\,. \tag{2.39}$$

Remark: Note that d is not subject to restrictions and does not depend on the input. Hence we can assume $d = 0$ by implicitly applying a phase space translation of $-d$ such that

$$T(\mathrm{W}_\xi) = \mathrm{W}_{\Gamma\cdot\xi}\, \mathrm{e}^{-g(\xi,\xi)/4}\,. \tag{2.40}$$

The exponential factor $t(\xi) = \exp\bigl(-g(\xi,\xi)/4 + \mathrm{i}\xi^{\mathrm{T}}\cdot d\bigr)$ is the characteristic function of a Gaussian state with respect to the »twisted« symplectic form $\Sigma = \sigma_{\mathrm{out}} - \Gamma^{\mathrm{T}}\sigma_{\mathrm{in}}\,\Gamma$, since g obeys the state condition

$$g + \mathrm{i}\Sigma \geq 0\,. \tag{2.41}$$

For a linear transformation Ω such that $\Sigma = \Omega^{\mathrm{T}}\cdot\sigma_{\mathrm{out}}\cdot\Omega$, t can be written as $t = \chi_T(\Omega\cdot\xi)$, where $\chi_T(\xi)$ is the characteristic function of a Gaussian state with respect to σ_{out}. For fixed Γ and Ω, this state characterizes the channel T.

Proof: While the complete proof can be found in [20], a brief sketch of the idea might be in order. Firstly, it suffices to show positivity on the dense subspace of the CCR algebra $\mathrm{ccr}(\Xi,\sigma)$ spanned by the Weyl operators and extensions by finite-dimensional matrix algebras. The »if«-part is proven by explicitly showing that T is completely positive. The »only if«-clause is checked by showing equivalence to the Bochner-Khinchin condition for t with respect to the »twisted« symplectic form Σ, i.e. for any number $n \in \mathbb{N}$ of phase space vectors $\xi_1, \xi_2, \ldots, \xi_n \in \Xi$ and coefficients $c_1, c_2, \ldots, c_n \in \mathbb{C}$

$$\sum_{k,l=1}^{n} c_k\,\overline{c_l}\,t(\xi_k - \xi_l)\,\exp\bigl(\mathrm{i}\Sigma(\xi_k,\xi_l)/2\bigr) \geq 0\,. \qquad \square$$

Note that Σ might be degenerate, i.e. have a nontrivial kernel. In this case, part of the function t describes a classical state. In particular, if $\sigma_{\mathrm{out}} = \sigma_{\mathrm{in}}$ and Γ is a symplectic transformation, $\Sigma = 0$ and the condition (2.39) reduces to $g \geq 0$. Then $g = 0$ is a possible choice for T to be completely positive.

Under the action of a channel T, the characteristic function $\chi(\xi)$ of a state ρ is transformed into $\chi'(\xi)$ according to

$$\begin{aligned}\chi'(\xi) &= \mathrm{tr}\bigl[T_*(\rho)\,\mathrm{W}_\xi\bigr] = \mathrm{tr}\bigl[\rho\,T(\mathrm{W}_\xi)\bigr] = \mathrm{tr}\bigl[\rho\,\mathrm{W}_{\Gamma\,\xi}\bigr]\,\mathrm{e}^{-g(\xi,\xi)/4+\mathrm{i}\xi^{\mathrm{T}}\cdot d}\\ &= \chi(\Gamma\,\xi)\,\mathrm{e}^{-g(\xi,\xi)/4+\mathrm{i}\xi^{\mathrm{T}}\cdot d}\,.\end{aligned}$$

Correspondingly, the covariance matrix γ of ρ changes as

$$\gamma \mapsto \Gamma^{\mathrm{T}}\cdot\gamma\cdot\Gamma + g\,.$$

The bilinear form g can be interpreted as additional noise which is necessary to turn a quasi-free map of the form (2.38) given by Γ into a completely positive map. Similar to the discussion of (2.22) and (2.24), this noise can be interpreted as arising from a convolution with a Gaussian distribution $\exp(-\xi^{\mathrm{T}}\cdot\sigma^{\mathrm{T}}\,g^{-1}\,\sigma\cdot\xi/4)$, cf. Eq. (2.25). However, since g corresponds to a quantum state by (2.41), the noise

is in general not purely classical. It can be split into a quantum contribution, which corresponds to the covariance matrix of a pure state with respect to (2.41), and a classical part given by a semidefinite-positive matrix. Due to the noise, a channel T from (2.38) is an irreversible operation unless $g = 0$. However, by (2.41) this requires $\Sigma = 0$ and thus $\sigma_{\text{out}} = \sigma_{\text{in}}$ and $\Gamma \in \mathrm{Sp}(2f, \mathbb{R})$; see above.

Completely positive linear maps can be represented by a set of Kraus operators $\{K_i\}$ [25] such that in the Schrödinger picture

$$T_*(\rho) = \sum_i K_i \, \rho \, K_i^* \,,$$

where $K_i \colon \mathcal{H} \to \mathcal{K}$ if $T_* \colon \mathcal{B}_*(\mathcal{H}) \to \mathcal{B}_*(\mathcal{K})$ and $\sum_i K_i \, K_i^* = \mathbb{1}$ for trace-preserving T_*. Conversely, every map of this form is completely positive. In the Heisenberg picture, the same Kraus operators are applied to the observable by (2.37),

$$T(A) = \sum_i K_i^* \, A \, K_i \,.$$

For composite systems, an important class of channels are the trace-preserving separable superoperators; these are represented by Kraus operators which factorize into a tensor product of operators on the subsystems: If such a channel T_* acts on a composite system with Hilbert space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$, the Kraus operators have the form $K_i = A_i \otimes B_i$, where the A_i act on $\mathcal{H}_A$ and the B_i on $\mathcal{H}_B$. For example, local operations with classical communication (LOCC) and in particular completely classical transformations have this form.

Cloning

3 Optimal cloners for coherent states

This chapter is concerned with optimizing the deterministic cloning of coherent states, i.e. the approximate duplication of such quantum states. A general feature of quantum physics is the impossibility of perfect duplication of an *unknown* quantum state. On the one hand, this is a direct consequence of the linear structure of quantum mechanics [1, 26, 27]. On the other hand, it is also related to a whole set of impossible tasks in quantum mechanics[1] [28]: Given two identical copies of the same quantum state, one could in principle obtain perfect measurement results for two noncommuting observables, which is impossible by virtue of a Heisenberg uncertainty [29]. However, it is possible to turn an unknown input quantum state and a fixed initial quantum state into two approximate duplicates of the input state. The quality of these clones is inversely related to each other: the better one resembles the input state, the worse does the other. This relation can be strictly quantified in terms of bounds on the cloning quality.

The field of quantum information has turned the impossibility of perfect cloning into a key feature of secure quantum communication, because it allows to detect essentially any eavesdropping on a transmission line from the degradation of the output. It is thus possible to give estimations of the security of the exchanged information, which is an important element of quantum key distribution (see e.g. [30,31,32,47] for QKD with coherent states). In addition, bounds on the cloning quality provide criteria to determine the validity of other protocols, since they cannot possibly imply a violation of these bounds. A positive example is given in Section 3.6, where we argue that violation of the cloning bounds necessarily implies certain success criteria for quantum teleportation.

A general cloning map, a »cloner«, turns m identical copies, i.e. an m-fold tensor product, of an input state into $n > m$ output states or »clones«, which resemble the input state. In contrast to the input state, the overall output state might contain correlations between the clones. The quality of the output states is measured in terms of a *figure of merit*, a functional which compares the output states to the input state. Usually, this is the fidelity, i.e. the overlap between input and output states. Depending on whether one considers individual clones or compares the joint output of the cloner with an n-fold tensor product of perfect copies of the input state, we call the respective figures of merit either *single-copy* or *joint* fidelity. In case the quality of the output states is identical, the cloner is called *symmetric*. It is *universal* if the quality of the clones does not depend on the input state.

The cloning of finite-dimensional pure states was investigated thoroughly, e.g. in [33,34,35,36,37,38,39]. Optimal universal cloners exist [33,34,35], which replicate

1 The impossibility of these tasks is not limited to quantum mechanics, but prevails in any nonsignaling theory with violation of Bell's inequalities.

all pure input states with equal fidelity. Remarkably, these cloners simultaneously maximize both the joint and the single-copy fidelity [39]. For continuous-variable systems, a universal cloner with finite fidelities for all pure input states cannot exist. As explained in Section 3.4.1 below, for every cloner there are pure squeezed states which yield a fidelity of zero. To facilitate handling of the mathematical structures, the set of input states is further restricted to Gaussian states, which are also important from a practical point of view (cf. the discussion in the Introduction). The set of pure, nonsqueezed Gaussian states is the set of coherent states, which we take as our input states. Similar to the finite-dimensional case, the cloning of coherent states was studied in depth, see [48,49,50,53,54,55] and references mentioned below. However, the cloners considered were restricted to Gaussian operations and were also assumed to be covariant with respect to phase space translations of the input state. It remained unclear if this set of cloners includes the optimal one. In particular, the results include a proof [55] that under this presumptions the best symmetric Gaussian 1-to-2 cloner is limited to a single-copy fidelity of $\frac{2}{3}$ as well as its optical implementation [48,49,50]. While mostly only deterministic cloners are studied, [51] investigates probabilistic finite-dimensional and continuous-variable cloning.

In the following we optimize the worst-case joint fidelities and weighted single-copy fidelities for deterministic 1-to-n cloning of coherent input states. These quantities do not depend on a priori information about the probability distribution of the input states (as long as all coherent states can occur). We show that the optimal fidelities can indeed be reached by cloners which are covariant with respect to phase space translation (Sec. 3.3). These cloners are necessarily quasi-free, i.e. they map Weyl operators onto multiples of Weyl operators in the Heisenberg picture (Sec. 3.3.2). Contrary to the finite-dimensional case, the optimization of single-copy and joint fidelity for coherent input states requires different cloners. While the joint fidelity is analytically maximized by a Gaussian cloner, the single-copy fidelity can be enhanced by non-Gaussian operations (Sec. 3.4.1, 3.4.2). For the case of a symmetric cloner which takes one copy of the input state into two clones, the maximal fidelity is approximately 0.6826, compared to $\frac{2}{3}$ for the best Gaussian cloner. We also analytically derive the best single-copy fidelities reached by Gaussian cloners for the 1-to-2 cloning with arbitrary weights and symmetric 1-to-n cloning. In addition, we show that classical cloning is limited to a fidelity of $\frac{1}{2}$ (Sec. 3.4.3). This can be reached by a Gaussian scheme, namely by a heterodyne measurement on the input state and repreparation of coherent states according to the measurement result. Furthermore, the fidelity cannot be enhanced by the use of supplemental PPT-bound entangled states. The results on cloning fidelities give rise to success criteria for continuous-variable teleportation. One of these criteria proves and extends an important conjecture in the literature (cf. Sec. 3.6).

The main results and arguments presented in this chapter have been published in [a].

3.1 Setup

A deterministic 1-to-n cloner abstractly is a completely positive, trace-preserving map which in the Schrödinger picture transforms a single input state into an output state of n subsystems, the clones. In the Heisenberg picture, these channels map observables on the output systems onto observables on the input system. Our task is to characterize these cloning maps and to optimize them with respect to suitable fidelities.

To more formally describe the class of relevant cloning maps, we start by setting up the involved phase spaces. If $\Xi_{\mathrm{in}} = \mathbb{R}^2$ denotes the phase space of the one-mode input system equipped with the nondegenerate symplectic form σ_{in}, then the output is described in terms of the phase space $\Xi = \bigoplus_{j=1}^{n} \Xi_{\mathrm{in}}$ with symplectic form

$$\sigma(\xi,\eta) = \sigma\Big(\bigoplus\nolimits_{j=1}^{n}\xi_j, \bigoplus\nolimits_{j=1}^{n}\eta_j\Big) = \sum_{j=1}^{n} \sigma_{\mathrm{in}}(\xi_j,\eta_j)\,.$$

Where appropriate, we identify a vector in Ξ with the n-tuple of its components in Ξ_{in}, i.e. $\Xi \ni \xi \equiv \bigoplus_{j=1}^{n} \xi_j \equiv (\xi_1,\ldots,\xi_n)$.

Recalling the discussion of Section 2, a channel between continuous-variable systems is a map between (states on) the respective CCR algebras. The cloning map T in the Heisenberg picture maps the output CCR algebra onto the input CCR algebra, i.e.

$$T\colon\ \mathrm{ccr}(\Xi,\sigma) \to \mathrm{ccr}(\Xi_{\mathrm{in}},\sigma_{\mathrm{in}})\,.$$

In the Schrödinger picture, the cloner T maps input states onto output states,

$$T_*\colon \mathcal{S}\big(\mathrm{ccr}(\Xi_{\mathrm{in}},\sigma_{\mathrm{in}})\big) \to \mathcal{S}\big(\mathrm{ccr}(\Xi,\sigma)\big)\,,$$

where $\mathcal{S}\big(\mathrm{ccr}(\Xi,\sigma)\big)$ denotes the state space of the CCR algebra. For general states, including singular states, this is the space of positive linear functionals on the representation Hilbert space $\mathcal{H}$, i.e. $\mathcal{S}\big(\mathrm{ccr}(\Xi,\sigma)\big) = \mathcal{B}^*(\mathcal{H})$. If only normal states are involved, it can be restricted to the space of trace class operators on $\mathcal{H}$, i.e. $\mathcal{S}\big(\mathrm{ccr}(\Xi,\sigma)\big) = \mathcal{B}_*(\mathcal{H})$. Due to the Stone-von Neumann Theorem 2.1, the representation Hilbert space is essentially unique: for $\mathrm{ccr}(\Xi_{\mathrm{in}},\sigma_{\mathrm{in}})$ and $\mathrm{ccr}(\Xi,\sigma)$ we have $\mathcal{H}_{\mathrm{in}} = \mathcal{L}^2(\mathbb{R}^2,\mathrm{d}x)$ and $\mathcal{H} = \mathcal{H}_{\mathrm{in}}^{\otimes n} \simeq \mathcal{L}^2(\mathbb{R}^{2n},\mathrm{d}x)$, respectively, where $\mathrm{d}x$ is understood to have appropriate dimension.

3.2 Fidelities

The fidelity quantifies how well two quantum states coincide [40, 41]. For general states described by density matrices ρ_1 and ρ_2, it is defined as

$$f(\rho_1,\rho_2) = \left(\mathrm{tr}\Big[\,\big(\rho_1^{1/2}\,\rho_2\,\rho_1^{1/2}\big)^{1/2}\,\Big]\right)^2.$$

If one of the states is pure, as in our case, this expression reduces to $f(\rho_1, \rho_2) = \mathrm{tr}[\rho_1\, \rho_2]$. We employ this functional to quantify the quality of the clones with respect to the input state.

For example, we could require that the overlap between the joint output $T_*(\rho)$ of the cloner and a tensor product of n perfect copies of the input state ρ becomes as large as possible. This is accomplished by maximizing the *joint fidelity*

$$f_{\mathrm{joint}}(T, \rho) = \mathrm{tr}\left[T_*(\rho)\, \rho^{\otimes n}\right]. \tag{3.1}$$

Since this criterion compares the complete output state, including correlations between subsystems, with a tensor product state, which is noncorrelated, it might be too strong. Instead, one could measure the quality of individual clones by comparing a single output subsystem, e.g. the i-th, to the input state with an appropriate fidelity expression:

$$f_i(T, \rho) = \mathrm{tr}\left[T_*(\rho)\, (\mathbb{1} \otimes \cdots \otimes \mathbb{1} \otimes \rho^{(i)} \otimes \mathbb{1} \cdots \otimes \mathbb{1})\right], \tag{3.2}$$

where the upper index (i) indicates the position in the tensor product. However, a single such »one-clone-only« fidelity could be trivially put to one by a cloner which does essentially nothing, but merely returns the input state in the i-th subsystem of the output and yields a suitable fixed stated for the other subsystems. So, optimizing the fidelities for all i in sequence would result in different cloners for each fidelity. To avoid this, we optimize over a weighted sum of such fidelities, $\sum_{i=1}^{n} \lambda_i\, f_i(T, \rho)$ with positive weights λ_i. The relative weights determine which clones should resemble the input state more closely and thus allow to describe nonsymmetric cloners.

For a similar reason it is not useful to optimize the cloner for each input state separately, because that would yield a source which perfectly produces the respective quantum state. Instead, we can either consider the average or the worst-case quality with respect to an ensemble of input states. However, both approaches face conceptual difficulties. In the first case, the process of averaging over the pure Gaussian states is not well defined, because this amounts to averaging over the group $\mathrm{Sp}(2n, \mathbb{R})$ of symplectic transformations, which is noncompact. In the latter case, for every given cloner squeezed states exist which for sufficiently large squeezing bring the fidelity arbitrarily close to zero (see end of Section 3.4.1). While this can in principle be compensated for a fixed and known squeezing by a modified cloner (desqueeze, clone unsqueezed state and resqueeze output), it is not possible to circumvent this behavior for arbitrary, unknown squeezing. We address the problem by optimizing the cloner only for coherent states, which constitute a subset of all pure Gaussian states.

As the figure of merit, we choose the worst-case fidelities $f_{\mathrm{joint}}(T)$ and $f_i(T)$, defined as the infima of (3.1) and (3.2) over the set $\mathrm{coh} = \left\{|\xi\rangle\langle\xi| \;\middle|\; \xi \in \Xi_{\mathrm{in}}\right\}$ of all coherent states,

$$f_{\mathrm{joint}}(T) = \inf_{\rho \in \mathrm{coh}} f_{\mathrm{joint}}(T, \rho) \quad \text{and} \quad f_i(T) = \inf_{\rho \in \mathrm{coh}} f_i(T, \rho).$$

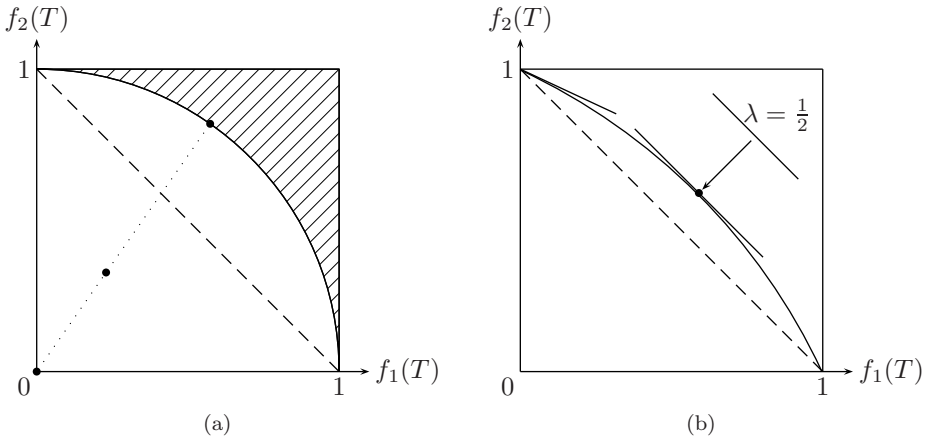


Figure 3.1:
Schematic diagram of the convex set f_{sc} of achievable worst-case single-copy fidelities for 1-to-2 cloning. Any fidelity pair between the origin and the arc (e.g. on the dotted line) can be realized by a classical mixture of an optimal cloner on the arc and a fixed output state, represented by the origin. The shaded area of fidelities is not accessible. The right diagram illustrates the interpretation of tangents. In contrast to (a), the optimal cloners in (b) are the trivial cloners for small values of λ or $(1-\lambda)$, indicated by the finite slope of the tangent in $(0,1)$ and $(1,0)$. See text for further details.

Therefore, our task is to find the maximal worst-case joint fidelity with respect to all cloners T,

$$f_{\text{joint}} = \sup_T f_{\text{joint}}(T) = \sup_T \inf_{\rho \in \text{coh}} f_{\text{joint}}(T, \rho)\,,$$

and the set f_{sc} of all achievable n-tuples $\big(f_1, f_2, \ldots, f_n\big)$ of worst-case single-copy fidelities.

This set is schematically depicted in Fig. 3.1 for the case of 1-to-2 cloning. Each point in the diagram corresponds to a pair of worst-case single-copy fidelities for the two clones in the output and thus to a cloner yielding these fidelities. The achievable fidelities are of course restricted by the requirement that $f_1 \leq 1$ and $f_2 \leq 1$. From two cloners one can construct a whole range of cloners by classical mixing; the resulting fidelities lie on the line connecting the fidelity pairs of the two initial cloners, indicated by the points on the dotted line. Consequently, the set f_{sc} is convex. The points with fidelities $(f_1, f_2) = (1,0)$ and $(0,1)$ represent the trivial cloners which return the input state in one output subsystem and leave the other in a fixed reference state. All fidelity pairs below and on the dashed line can be reached by a classical mixture of these cloners and a fixed output state, represented by the origin with $(f_1, f_2) = (0,0)$. Optimizing cloners has the effect of enlarging the convex

area of achievable fidelity pairs. The optimal cloners yield fidelities corresponding to points on the »high fidelity« rim of this set, schematically indicated by the arcs in Fig. 3.1. Any 1-to-2 cloning fidelity pair allowed by quantum physics can be reached by classically mixing an optimal cloner with a fixed output state (depicted by the dotted line). The fidelities beyond the curve of optimal cloners are not accessible (indicated in Fig. 3.1(a) by the shaded region).

An additional aspect of the interpretation of the diagrams is provided by the tangents, depicted by the thin solid lines in Fig. 3.1(b). Following from the total weighted single-copy fidelity for 1-to-2 cloning, $f = \lambda f_1 + (1-\lambda) f_2$, all cloners on the line $f_2 = f/(1-\lambda) - f_1 \lambda/(1-\lambda)$ yield the total fidelity f for weight λ. Conversely, a line with slope $s = -\lambda/(1-\lambda)$ and abscissa $t = f/(1-\lambda)$ comprises all cloners yielding f for weight λ. Moving a line with slope s parallel to itself until it touches the set f_{sc} results in the optimal cloner for the corresponding weight (the dot in Fig. 3.1(b) for $\lambda = \frac{1}{2}$). Moreover, the slope of the tangent in $(0,1)$ and $(1,0)$ conveys important information about the optimality of the trivial cloners, which solely map the input state into one of the two output subsystems. If the line with slope corresponding to some $\lambda_0 > 0$ touches the curve of optimal cloners in $(0,1)$, the optimal cloner for weight λ_0 is the trivial cloner with $(f_1, f_2) = (0,1)$, degraded by a fixed output state $(f_1, f_2) = (0,0)$ with weight λ_0 and total fidelity $f = (1-\lambda_0)$. This is illustrated in Fig. 3.1(b). In contrast, Fig. 3.1(a) corresponds to a case where the trivial cloners are optimal only for $\lambda = 0$ and $\lambda = 1$, since the tangent in the end points of the arc is horizontal or vertical.

Since we show below that the optimal worst-case fidelities can be reached by cloners which are covariant with respect to phase space translations of the input state, we simultaneously optimize the average fidelities.

3.3 Covariance

In this section, we will show that for every cloner we can define a cloner which is covariant with respect to translations of the input state in phase space and which yields at least the same worst-case fidelity for coherent input states. For 1-to-n cloning, such cloners are necessarily quasi-free, i.e. they map Weyl operators to multiples of Weyl operators, and are essentially determined by a state on the output CCR algebra.

A map on states is phase space covariant in the above sense if displacing the input state in phase space gives the same result as displacing the output by the same amount. If we define the shifted cloner T_ξ by

$$T_{*\xi}(\rho) = \mathrm{W}_\xi^{\otimes n\,*}\, T_*(\mathrm{W}_\xi\, \rho\, \mathrm{W}_\xi^*)\; \mathrm{W}_\xi^{\otimes n}\,, \tag{3.3}$$

translational covariance means $T_{*\xi}(\rho) = T_*(\rho)$. Note that the same phase space translation ξ is used for the input system as well as for all output subsystems. This is justified from the intention to replicate the input state as closely as possible. Given covariance of T_* in the Schrödinger picture, the covariance of T in the Heisenberg picture follows immediately: If T_* is covariant with respect to phase space translations,

the expectation value of an arbitrary observable A in a state ρ obeys

$$\begin{aligned}\operatorname{tr}\big[\rho\, T(A)\big] = \operatorname{tr}\big[T_*(\rho)\, A\big] &= \operatorname{tr}\big[\mathrm{W}_\xi^{\otimes n^*}\, T_*(\mathrm{W}_\xi\, \rho\, \mathrm{W}_\xi^*)\, \mathrm{W}_\xi^{\otimes n}\, A\big] \\ &= \operatorname{tr}\big[\rho\ \mathrm{W}_\xi^*\, T(\mathrm{W}_\xi^{\otimes n} A\, \mathrm{W}_\xi^{\otimes n^*})\, \mathrm{W}_\xi\big]\,.\end{aligned} \tag{3.4}$$

Thus, covariance of T follows from covariance of T_* and we will in the following use the one or the other interchangeably. Using T, the fidelities can be written in a unified form as $f(T,\rho) = \operatorname{tr}[\rho\, T(A)]$, where $A = \rho^{\otimes n}$ and $A = \sum_i \lambda_i\, \mathbb{1}\otimes\cdots\otimes\mathbb{1}\otimes\rho^{(i)}\otimes\mathbb{1}\cdots\otimes\mathbb{1}$ for $f = f_{\text{joint}}$ and $f = \sum_i \lambda_i\, f_i$, respectively. Furthermore, for coherent states we get

$$\begin{aligned} f\big(T, |\xi\rangle\langle\xi|\big) &= \operatorname{tr}\big[|0\rangle\langle 0|\, T_\xi(A)\big] = f\big(T_\xi, |0\rangle\langle 0|\big)\,, \text{ where} \\ T_\xi(A) &= \mathrm{W}_\xi^*\ T\big(\mathrm{W}_\xi^{\otimes n} A\, \mathrm{W}_\xi^{\otimes n^*}\big)\, \mathrm{W}_\xi \end{aligned}$$

in strict analogy with (3.3).

By applying an average M_ξ over the symmetry group of phase space translations, we can define for every map T a covariant map which we denote by $\widetilde{T}_\xi$. However, since the group of translations is noncompact, M_ξ has to be an »invariant mean« [42] which does exist only by virtue of the Axiom of Choice. The cloner $\widetilde{T}_\xi$ yields worst-case fidelities which are not lower than those achieved by T [43]. For a discussion, see the proof of

Lemma 3.1:
For every 1-to-n cloner T there exists a covariant cloner $\widetilde{T}_\xi$ such that for $f = f_{\text{joint}}$ or $f = \sum_i \lambda_i\, f_i$

$$f(T) \le f(\widetilde{T}_\xi)\,.$$

Remark: The cloner $\widetilde{T}_\xi$ might be »singular«, i.e. its output for normal states described by a density operator ρ could be a purely singular state, which cannot be connected to any density operator. This issue is addressed in the next Section 3.3.1, where it is shown that such cloners are not optimal.

Proof: The invariant mean M_ξ will not be applied to T directly but to bounded phase space functions $g(\xi)$, where $\mathsf{M}_\xi\big[g(\xi)\big]$ is linear in g, positive if g is positive, normalized as $\mathsf{M}_\xi[1] = 1$ and indifferent to translations, $\mathsf{M}_\xi\big[g(\xi+\eta)\big] = \mathsf{M}_\xi\big[g(\xi)\big]$. For expectation functionals of a bounded operator A on the cloner output $T_{*\xi}(\rho)$, the invariant mean $\mathsf{M}_\xi \operatorname{tr}\big[T_{*\xi}(\rho)\, A\big]$ is well-defined as the argument is a function bounded by $\|A\|$. Moreover, by the properties of M_ξ it is a covariant, bounded, normalized, positive linear functional on A, which describes a state on the output CCR algebra. Since it is also linear in ρ, we can introduce a linear operator $\widetilde{T}_*$ such that $\widetilde{T}_*(\rho)$ is the respective state. However, this state might be singular (see Section 3.3.1 below), hence $\widetilde{T}_*$ has to map density operators of the input system onto the linear functionals on the output CCR algebra:

$$\begin{aligned} &\widetilde{T}_*(\rho)\colon \mathcal{B}_*(\mathcal{H}) \to \mathcal{B}^*(\mathcal{H}^{\otimes n})\,, \text{ such that} \\ &\widetilde{T}_*(\rho)[A] = \mathsf{M}_\xi \operatorname{tr}\big[T_{*\xi}(\rho)\, A\big]\,. \end{aligned}$$

By (3.1) and (3.2), joint and single-copy fidelity for the shifted cloner T_ξ are bounded phase space functions to which we can apply M_ξ. For $f = f_{\text{joint}}$ or $f = \sum_i \lambda_i f_i$, this yields the relations

$$\begin{aligned} f(T) &= \inf_\xi f\big(T, |\xi\rangle\langle\xi|\big) = \inf_\xi f\big(T_\xi, |0\rangle\langle 0|\big) \\ &\leq \mathsf{M}_\xi\, f\big(T_\xi, |0\rangle\langle 0|\big) = f\big(\widetilde{T}_\xi, |0\rangle\langle 0|\big) = f(\widetilde{T}_\xi)\,. \end{aligned}$$

The first equality is the definition of $f(T)$ from Eqs. (3.1, 3.2), the second corresponds to $f\big(T, |\xi\rangle\langle\xi|\big) = f\big(T_\xi, |0\rangle\langle 0|\big)$. The inequality is due to the fact that the minimum of a function is less than or equal to its average. As discussed above, the averaged fidelity can be attributed to a cloner which is denoted by $\widetilde{T}_\xi$. Moreover, $\widetilde{T}_\xi$ is covariant and thus yields constant fidelities for all coherent input states. Consequently, the function $\eta \mapsto f\big(\widetilde{T}_\xi, |\eta\rangle\langle\eta|\big)$ is constant for this cloner and the worst-case fidelity as the infimum over η is attained for any η. □

This lemma assures that for every cloner T the averaging, covariant cloner $\widetilde{T}_\xi$ is at least as good as the initial map T with respect to joint and single-copy fidelity. Therefore, we can restrict the optimization to covariant cloners in the first place, which yield constant fidelities for all coherent input states.

3.3.1 Technicalities

While the averaging cloner $\widetilde{T}_\xi$ does exist, care must be taken in employing it. The output states of such a cloner might be singular, i.e. a functional on the observables which cannot be described by a density operator. Consider for example a »cloner« which outputs a constant normal state, $T_*(\rho) = \rho_0$. This cloner can be turned into a covariant cloner $\widetilde{T}_*$ by applying the invariant mean from above. The output $\widetilde{T}_*(\rho)$ is a constant, translationally invariant state. However, it is purely singular since there cannot be a translationally invariant density operator as the following argument shows: Assume the density operator ρ_0 were covariant with respect to all phase space translations. Then one would expect that for all $\xi \in \Xi$

$$\operatorname{tr}[\rho_0\, A] = \operatorname{tr}\big[\rho_0\ \mathrm{W}_\xi\, A\, \mathrm{W}_\xi^*\big] = \operatorname{tr}\big[\mathrm{W}_\xi^*\, \rho_0\, \mathrm{W}_\xi\, A\big]\,, \tag{3.5}$$

which can only be true if ρ_0 commutes with all Weyl operators W_ξ. Since the Weyl system is supposed to be irreducible, this implies $\rho_0 \propto \mathbb{1}$, which is not a trace class operator and thus cannot constitute a density operator.

However, a purely singular output state yields fidelity zero for the cloner, since both single-copy and joint fidelity, $f = f_{\text{joint}}$ or $f = \sum_j \lambda_j f_j$, of a cloner can be written as expectation values of compact operators F_{joint} and F_i in the output state of the cloner. In particular, for covariant cloners and coherent input states we can restrict attention to tensor products of compact operators of the form $|\alpha\rangle\langle\alpha|$ with itself or the identity operator: $F_{\text{joint}} = |\alpha\rangle\langle\alpha|^{\otimes n}$ and $F_i = \mathbb{1} \otimes \cdots \otimes \mathbb{1} \otimes |\alpha\rangle\langle\alpha|^{(i)} \otimes \mathbb{1} \otimes \cdots \otimes \mathbb{1}$ (where the upper index denotes the number of the tensor factor, i.e. the

clone). A more general type of cloner yields normal output on some of the clones and a singular state on the rest, i.e.

$$T_*(\rho) = (T_{*\Lambda} \otimes \widetilde{T}_{*\Lambda^c})(\rho)\,, \tag{3.6}$$

where $T_{*\Lambda}$ is a normal cloner on the clones indicated by $\Lambda \subset \{1, 2, \ldots, n\}$ and $\widetilde{T}_{*\Lambda^c}$ is a purely singular cloner on the rest. The following lemma shows that cloners which contain purely singular parts in the output are not optimal:

Lemma 3.2:
For covariant 1-to-n cloners optimized with respect to worst-case single-copy or joint fidelity, the following holds:

(i) A cloner with a purely singular contribution to the output state cannot be optimal. The optimal cloner is a linear combination of covariant cloners which yield a normal state for some of the clones and purely singular output for the rest, i.e. a linear combination of the cloners in (3.6).

(ii) For joint fidelity, the optimal cloner is normal.

(iii) If the cloner is to be covariant with respect to more clones than enter the fidelity criterion, then the optimal cloner is singular.

Remark: If the weighted single-copy fidelity $f = \sum_{i=1}^{n} \lambda_i f_i$ contains terms with $\lambda_i = 0$, these clones do not enter the fidelity criterion but formally require a 1-to-n cloner which is covariant with respect to all n clones. In this case, the proof shows that the optimal cloner is either not covariant for all clones or singular. We cope with this issue by disregarding clones with $\lambda_i = 0$. Instead, we consider a cloner which is restricted to the clones with $\lambda_i \neq 0$. For the only exception, see the following Corollary 3.3.

Proof: The proof follows [43]. In general, a state ω is a positive linear functional on the algebra of observables, i.e. $\omega \in \mathcal{B}(\mathcal{H}^{\otimes f})$, cf. Section 2.2.4. However, since we are only interested in expectation values for fidelities, we can restrict states to a specially tailored subalgebra. For a single system, we define $\mathcal{D} \subset \mathcal{B}(\mathcal{H})$ as the algebra of all operators of the form

$$D = C + d\,\mathbb{1}\,, \text{ yielding expectation values } \omega(D) = \omega(C) + \omega(\mathbb{1})\,d\,, \tag{3.7}$$

where C is a compact operator on $\mathcal{H}$ and $d \in \mathbb{C}$. This definition separates contributions to the expectation value from normal and purely singular parts of a state ω: Since a purely singular state ω' yields an expectation value of zero on compact operators, the parameter d can be obtained as $d = \omega'(C + d\,\mathbb{1})$ from any such state. The decomposition (3.7) is thus unique. Hence any state ω on $\mathcal{D}$ consists of two parts: a linear functional on the compact operators, which necessarily corresponds to a (nonnormalized) density operator ω_1 by $\omega(C) = \mathrm{tr}[\omega_1\, C]$, and a term proportional to d, which introduces another parameter $\omega_0 \in \mathbb{R}$. Expectation values of ω are thus given by

$$\omega(D) = \omega(C) + \omega(\mathbb{1})\,d = \mathrm{tr}[\omega_1\, C] + d\,\big(\mathrm{tr}[\omega_1] + \omega_0\big)\,. \tag{3.8}$$

Normalization of ω imposes $\omega(\mathbb{1}) = \mathrm{tr}[\omega_1]+\omega_0 = 1$ and positivity requires that $\omega_0 \geq 0$ and $\omega_1 \geq 0$. An intuitive interpretation would suggest that ω_0 is the probability for a system in state ω to be »at infinity«,[2] while $\omega_1/(1-\omega_0)$ is the normalized density operator describing the nonsingular part of ω. Note that the fidelity of ω with respect to a coherent state α is determined by the compact operator $|\alpha\rangle\langle\alpha|$ as

$$f\big(\omega, |\alpha\rangle\langle\alpha|\big) = \omega\big(|\alpha\rangle\langle\alpha|\big) = \mathrm{tr}\big[\omega_1|\alpha\rangle\langle\alpha|\big]\,, \tag{3.9}$$

which is independent of ω_0. Hence one can expect that the optimization of the cloner output state reduces the weight at infinity ω_0.

In order to obtain a more rigorous argument, we introduce the tensor product subalgebra $\mathcal{D}^{\otimes n} \subset \mathcal{B}\big(H^{\otimes n}\big)$ generated by the identity as well as all operators of the form $\mathbb{1}\otimes\cdots\mathbb{1}\otimes C\otimes\mathbb{1}\cdots\otimes\mathbb{1}$ which have a compact operator C in a single tensor factor. A product of such operators is characterized by the set $\Lambda \subset \Lambda_n = \{1,2,\ldots,n\}$ of tensor factors with compact entry; the complement $\Lambda^{\mathrm{c}} = \Lambda_n \setminus \Lambda$ contains a factor $\mathbb{1}^{\otimes\Lambda^{\mathrm{c}}}$. A general element $D \in \mathcal{D}^{\otimes n}$ is thus decomposed according to

$$D = \sum_{\Lambda} D_\Lambda \otimes \mathbb{1}^{\otimes\Lambda^{\mathrm{c}}}, \tag{3.10}$$

where D_Λ is the respective compact part on the tensor factors indexed by Λ and the sum runs over all subsets of Λ_n. Similarly, a state ω is decomposed into parts which are labeled by a set of tensor factors Λ on which the state is normal and thus described by a density operator ω_Λ; on the complement Λ^{c}, the part describes systems »at infinity«. The purely singular contribution is denoted by $\omega_\emptyset$. A part ω_Λ yields nonzero expectation value for D from (3.10) only on terms $D_{\Lambda'}\otimes\mathbb{1}^{\otimes\Lambda'^{\mathrm{c}}}$ for which $\Lambda' \subset \Lambda$ because else a singular part would meet a compact operator. Hence

$$\omega(D) = \omega\Big(\textstyle\sum_{\Lambda'} D_{\Lambda'}\otimes\mathbb{1}^{\otimes\Lambda'^{\mathrm{c}}}\Big) = \displaystyle\sum_{\Lambda}\sum_{\Lambda'\subset\Lambda} \mathrm{tr}\Big[\omega_\Lambda\big(D_{\Lambda'}\otimes\mathbb{1}^{\otimes\Lambda\setminus\Lambda'}\big)\Big]\,. \tag{3.11}$$

Positivity of ω is assured if all $\omega_\Lambda \geq 0$ and normalization requires $\sum_\Lambda \mathrm{tr}[\omega_\Lambda] = 1$.

This relation implies that the fidelity of the i-th clone with ω is obtained as

$$\omega(F_i) = \sum_{\Lambda\ni i} \mathrm{tr}\big[\omega_\Lambda\, F_i|_\Lambda\big]\,, \tag{3.12}$$

where the sum runs over all Λ containing the index i and $F_i|_\Lambda$ is the restriction of F_i to the tensor factors Λ. For a weighted sum of such fidelities, determined by $F(\lambda) = \sum_i \lambda_i F_i$ with $\lambda_i \geq 0$, the expectation value is given by a sum over the above expression,

$$\omega\big(F(\lambda)\big) = \sum_{\Lambda} \mathrm{tr}\Big[\omega_\Lambda\, F(\lambda)\big|_\Lambda\Big]\,. \tag{3.13}$$

2 This interpretation can be made rigorous by a correspondence between spaces of functions and spaces of operators, which allows a »one-point compactification« of the phase space, i.e. the process of adjoining a point at infinity to the real vector space. By using only a single point at infinity we identify all purely singular states, which is justified since they do not contribute to fidelities as explained above. This is a main motivation in the definition of $\mathcal{D}$.

In the case of joint fidelity, the respective expression contains only $\omega_{\Lambda_n}(F_{\text{joint}})$ since $F_{\text{joint}} = |\alpha\rangle\langle\alpha|^{\otimes n}$ is compact on all tensor factors.

To investigate the fidelities of a possibly singular, covariant cloner $\widetilde{T}_*$, consider the restriction $\omega = \widetilde{T}_*(\rho)|_{\mathcal{D}^{\otimes n}}$ of its output to $\mathcal{D}^{\otimes n}$. Denote by $\widetilde{T}_{*\Lambda}$ the map which takes the density operator ρ on $\mathcal{H}$ to $\widetilde{T}_{*\Lambda}(\rho) = \omega_\Lambda$, the unique density operator on the tensor factors Λ from the decomposition of ω. Since $\widetilde{T}_*$ is covariant, so is $\widetilde{T}_{*\Lambda}$. However, it lacks normalization, as only the overall $\widetilde{T}_*(\rho)$ is normalized. To renormalize $\widetilde{T}_{*\Lambda}$, we introduce the normalization operator N_Λ which implements the bounded linear map $\rho \mapsto \operatorname{tr}\big[\widetilde{T}_{*\Lambda}(\rho)\big] = \operatorname{tr}[\rho\, N_\Lambda] \leq 1$. As $\widetilde{T}_{*\Lambda}$ is covariant, N_Λ has to commute with all Weyl operators and is thus a multiple of the identity, $N_\Lambda = p_\Lambda\, \mathbb{1}$ with $0 < p_\Lambda \leq 1$. We define by

$$T_{*\Lambda}(\rho) = \widetilde{T}_{*\Lambda}(\rho)/p_\Lambda = \omega_\Lambda/p_\Lambda \tag{3.14}$$

a family of normalized, covariant 1-to-$|\Lambda|$ cloning transformations, where $|\Lambda|$ denotes the number of elements in the set Λ. Note that the normalization constant p_Λ does not depend on the input state. $T_{*\Lambda}(\rho)$ is *normal*, since the output ω_Λ/p_Λ is a density operator. With the help of $T_{*\Lambda}$, the fidelity of possibly singular cloners can be expressed in terms of nonsingular cloners. For joint fidelity, we get:

$$\begin{aligned}
f_{\text{joint}}\big(\widetilde{T}_*\big) &= f_{\text{joint}}\big(\widetilde{T}_*, |0\rangle\langle 0|\big) && \text{by covariance of } \widetilde{T}_* \\
&= \omega(F_{\text{joint}}) && \text{for } \omega = \widetilde{T}_*\big(|0\rangle\langle 0|\big) \\
&= \operatorname{tr}\big[\omega_{\Lambda_n}\, F_{\text{joint}}\big] && \text{by (3.11), } F_{\text{joint}} \text{ is compact on } \Lambda_n \\
&= p_{\Lambda_n}\, \operatorname{tr}\Big[T_{*\Lambda_n}\big(|0\rangle\langle 0|\big)\, F_{\text{joint}}\Big] && \text{by (3.14)} \\
&= p_{\Lambda_n}\, f_{\text{joint}}(T_{\Lambda_n}) && \text{by (3.1).}
\end{aligned}$$

Since $0 < p_\Lambda \leq 1$, this fidelity is enlarged if $p_{\Lambda_n} = 1$ and hence $p_\Lambda = 0$ for $\Lambda \neq \Lambda_n$, i.e. if $\widetilde{T}_* = T_{*\Lambda_n}$. But this better cloner is covariant and *normal*, which proves (ii) and (i) for joint fidelity, where the linear combination consists of a single covariant cloner which yields normal output for all clones.

For a proof of (iii), we discuss the role of zero and nonzero coefficients λ_i in the weighted single-copy fidelity $\sum_{i=1}^n \lambda_i\, f_i$. If one of the weights is zero, e.g. $\lambda_n = 0$, the figure of merit does not care for the respective clone n. A 1-to-n cloner can thus be optimized by using the optimal, covariant 1-to-$(n-1)$ cloner and amending the output with an arbitrary state for the n-th output system. However, if this additional state is a normal state, the resulting cloner is not covariant (see above). If this cloner is subjected to the averaging procedure from Lemma 3.1, the averaged cloner will be covariant and hence the state of the n-th clone in its output will be singular. Consequentially, if a clone is not contained in the figure of merit, the optimal cloner is either not covariant with respect to all clones or it is covariant but singular. This proves (iii).

Consider now the single-copy fidelity with nonzero weights $\lambda_i > 0$. We denote the respective fidelity operator by $F(\lambda) = \sum_i \lambda_i\, F_i$, where $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_n)$. With

this,

$$\begin{aligned} f\big(\widetilde{T}_*\big) &= f\big(\widetilde{T}_*, |0\rangle\langle 0|\big) && \text{by covariance of } \widetilde{T}_* \\ &= \omega\big(F(\lambda)\big) && \text{for } \omega = \widetilde{T}_*\big(|0\rangle\langle 0|\big) \\ &= \sum_\Lambda \mathrm{tr}\Big[\omega_\Lambda\, F(\lambda)\big|_\Lambda\Big] && \text{by (3.11)} \\ &= \sum_\Lambda p_\Lambda\ \mathrm{tr}\Big[T_{*\Lambda}\big(|0\rangle\langle 0|\big)\, F(\lambda)\big|_\Lambda\Big] && \text{by (3.14),} \end{aligned}$$

where $F(\lambda)|_\Lambda$ is the restriction of $F(\lambda)$ to tensor factors Λ. The normal output states of the cloners $T_{*\Lambda}$ can be amended with a constant, translationally invariant and thus purely singular state on Λ^c. This proves (i) for single-copy fidelity. □

This lemma leaves the possibility that cloners optimal with respect to weighted single-copy fidelities are singular. For the case of 1-to-2 cloning, this is ruled out from the results, see Section 3.4.2.

While we are nearly always interested in covariant nonsingular cloners, there is one exception: 1-to-n cloners which output the *exact* input state in one of the clones, or »copy-through« cloners. They occur as extremal cases in the optimization of weighted single-copy fidelities $\sum_i \lambda_i f_i$ if $\lambda_i = 0$ for $i \neq j$ but $\lambda_j \neq 0$. Optimal cloners of this type effectively copy the input state to the j-th output system and yield a respective fidelity of one. By the above Lemma 3.2, they are either not covariant with respect to all n clones or singular:

Corollary 3.3:
The covariant 1-to-n »copy-through« cloners, i.e. those cloners which output the *exact* input state in one of the clones, are singular. In fact, they are cloners of type (3.6) with $\Lambda = \{i\}$ for perfect replication of the input in the i-th clone:

$$T_*(\rho) = (T_{*\{i\}} \otimes \widetilde{T}_{*\Lambda^c})(\rho)\,.$$

3.3.2 Characterization

The characterization of covariant cloning maps is best carried out in the Heisenberg picture, where the cloner $T\colon \mathrm{ccr}(\Xi, \sigma) \to \mathrm{ccr}(\Xi_{\mathrm{in}}, \sigma_{\mathrm{in}})$ maps operators in the output CCR algebra to the input CCR algebra. Since the Weyl operators are eigenvectors of the phase space translation operation, $\mathrm{W}_\eta^*\, \mathrm{W}_\xi\, \mathrm{W}_\eta = \mathrm{e}^{-\mathrm{i}\sigma(\xi,\eta)}\, \mathrm{W}_\xi$ according to Eq. (2.7b), the covariance property takes on a particularly simple form for these operators. Moreover, since they give rise to a dense subset of the whole algebra, it is sufficient to assure covariance for an arbitrary Weyl operator.

In strict analogy to Eq. (3.3) and according to Eq. (3.4), covariance with respect to phase space translations for T is understood as

$$\begin{aligned} \mathrm{W}_\eta\, T(\mathrm{W}_{\xi_1,\ldots,\xi_n})\, \mathrm{W}_\eta^* &= T(\mathrm{W}_\eta^{\otimes n}\, \mathrm{W}_{\xi_1,\ldots,\xi_n}\, \mathrm{W}_\eta^{\otimes n *}) \\ &= \exp\big(\mathrm{i} \textstyle\sum_{j=1}^n \sigma_{\mathrm{in}}(\xi_j, \eta)\big)\, T(\mathrm{W}_{\xi_1,\ldots,\xi_n})\,, \end{aligned} \tag{3.15}$$

where the second identity is due to the Weyl commutation relation (2.7b). As $T(\mathrm{W}_{\xi_1,\ldots,\xi_n})$ is thus an eigenvector of all phase space translations $\eta \in \Xi$, Lemma 2.2 requires that it is a multiple of an appropriate Weyl operator,

$$T(\mathrm{W}_{\xi_1,\ldots,\xi_n}) = t(\xi_1,\ldots,\xi_n)\ \mathrm{W}_{\sum_i \xi_i}\,,$$

where t is a functional on the output phase space, $t\colon \Xi \to \mathbb{C}$. Since T maps Weyl operators to multiples of Weyl operators, it is quasi-free. In terms of characteristic functions of input and output states, this functional t acts as the characteristic function of the cloner itself:

$$\begin{aligned}\chi_{\mathrm{out}}(\xi_1,\ldots,\xi_n) &= \mathrm{tr}\big[T_*(\rho)\,\mathrm{W}_{\xi_1,\ldots,\xi_n}\big] = \mathrm{tr}\big[\rho\,T(\mathrm{W}_{\xi_1,\ldots,\xi_n})\big]\\ &= t(\xi_1,\ldots,\xi_n)\,\chi_{\mathrm{in}}(\textstyle\sum_i \xi_i)\,.\end{aligned} \tag{3.16}$$

For T to be completely positive and χ_{out} to describe a quantum state, t has to fulfill the condition stated in Theorem 2.6, i.e. it has to be the characteristic function of a state with respect to the CCR algebra over the output phase space (Ξ, Σ) equipped with the »twisted« symplectic form Σ [20]. In the case of 1-to-n cloning,

$$\Sigma(\xi,\eta) = \sigma(\xi,\eta) - \sigma_{\mathrm{in}}(\textstyle\sum_{j=1}^n \xi_j, \sum_{k=1}^n \eta_k) = \sigma(\Omega\,\xi, \Omega\,\eta)$$

for a suitable linear transformation Ω. A possible choice for this operator is to change momentum coordinates into positions, $p_j \mapsto q_j$, and position coordinates according to $q_j \mapsto \sum_{k\neq j} p_k$. For details on Ω, see the end of this section.

Using Ω, the above condition on t is equivalent to $t(\xi) = \chi_T(\Omega\,\xi)$ where $\chi_T(\xi)$ is the characteristic function of a state ρ_T with respect to $\sigma(\xi,\eta)$, i.e.

$$t(\xi) = \mathrm{tr}[\rho_T\,\mathrm{W}_{\Omega\,\xi}] = \chi_T(\Omega\,\xi)\,. \tag{3.17}$$

Hence, given Ω, a (deterministic) covariant cloner is completely described by the state ρ_T. The cloner is Gaussian if and only if it maps Gaussian states to Gaussian states and consequently if and only if $\chi_T(\xi)$ is a Gaussian function. For later reference, we state the characteristic function of the output explicitly:

$$\chi_{\mathrm{out}}(\xi_1,\ldots,\xi_n) = \chi_T(\Omega\,\xi)\,\chi_{\mathrm{in}}(\textstyle\sum_i \xi_i)\,. \tag{3.18}$$

The above results are summarized in the following

Proposition 3.4:
For every 1-to-n cloner T', there is a cloner T covariant with respect to phase space translations in the sense of Eq. (3.3) which on coherent states yields constant fidelities not less than the worst-case fidelities of T'. The cloner T is quasi-free and described by a state ρ_T with characteristic function $\chi_T(\xi)$ such that

$$T(\mathrm{W}_\xi) = \chi_T(\Omega\,\xi)\ \mathrm{W}_{\sum_i \xi_i}$$

for a fixed Ω satisfying $\sigma(\Omega\,\xi, \Omega\,\eta) = \sigma(\xi,\eta) - \sigma_{\mathrm{in}}(\sum_{j=1}^n \xi_j, \sum_{k=1}^n \eta_k)$.

Transformation Ω

In (Q,P)-block representation and with a square matrix $(\mathbb{E}_n)_{i,j} = 1$ for $i,j = 1,2,\ldots,n$ we have

$$\Sigma(\xi,\eta) = \xi^{\mathrm{T}} \cdot \begin{pmatrix} 0 & \mathbb{1}_n - \mathbb{E}_n \\ \mathbb{E}_n - \mathbb{1}_n & 0 \end{pmatrix} \cdot \eta = \sigma(\Omega\,\xi, \Omega\,\eta) \quad \text{choosing}^3$$

$$\Omega = \begin{pmatrix} 0 & \mathbb{E}_n - \mathbb{1}_n \\ \mathbb{1}_n & 0 \end{pmatrix}. \tag{3.19}$$

For later use, we compute $\det\Omega = (-1)^n\,(\det\mathbb{1}_n)\det(\mathbb{E}_n - \mathbb{1}_n)$. Since we will also need the eigenvalues of $\mathbb{E}_n$, we more generally compute its characteristic polynomial $\det(\mathbb{E}_n - \lambda\,\mathbb{1}_n)$. By inspection, we find the recursion relation

$$\det(\mathbb{E}_n - \lambda\,\mathbb{1}_n) = (2-\lambda-n)\,\det(\mathbb{E}_{n-1} - \lambda\,\mathbb{1}_{n-1}) + (n-1)\,\lambda\,\det(\mathbb{E}_{n-2} - \lambda\,\mathbb{1}_{n-2})$$

and prove by induction that

$$\det(\mathbb{E}_n - \lambda\,\mathbb{1}_n) = (-1)^n\,\lambda^n\,(\lambda - n)\,. \tag{3.20}$$

Letting $\lambda = 1$, this yields

$$\det\Omega = 1 - n\,. \tag{3.21}$$

The inverse of Ω is

$$\Omega^{-1} = \begin{pmatrix} 0 & \mathbb{1}_n \\ \mathbb{E}_n/(n-1) - \mathbb{1}_n & 0 \end{pmatrix}. \tag{3.22}$$

3.4 Optimization

A key ingredient of our optimization method is the linearity of the fidelities in T and hence in ρ_T. Using again the abbreviation $f = f_{\text{joint}}$ or $f = \sum_i \lambda_i\,f_i$, we can thus write the fidelity as the expectation value of a linear operator F in the state ρ_T:

$$f(T,\rho) = \mathrm{tr}[\rho_T\,F]\,. \tag{3.23}$$

The applicable operators $F = F_{\text{joint}}$ and $F = \sum_i \lambda_i\,F_i$ are obtained by expressing the fidelity in terms of characteristic functions by noncommutative Fourier transform and the Parseval relation (2.11), regrouping the factors and transforming back to new operators[4] ρ_T and F. The latter depends only on the symplectic geometry via the transformation Ω mediating between symplectic forms, but not on the cloner T. In principle, F also depends on the input state ρ. However, since we can restrict the

3 This choice is not unique, but can involve arbitrary symplectic transformations, i.e. $S^{-1}\,\Omega\,S$ for $S \in \mathrm{Sp}(2n,\mathbb{R})$ is permissible, too.

4 A similar method has been used independently by Wódkiewicz et al. to obtain results on the teleportation of continuous-variable systems [60] and the fidelity of Gaussian channels [61].

search to covariant cloners of coherent states, the worst-case fidelity is attained for any input state and we can fix the input state to the vacuum, $\rho = |0\rangle\langle 0|$:

$$f(T) = \inf_{\rho \in \mathrm{coh}} f(T, \rho) = f(T, |0\rangle\langle 0|)\,.$$

Maximizing the fidelity by taking the supremum of Eq. (3.23) over all covariant cloners is therefore equivalent to finding the state ρ_T that maximizes the above expectation value, i.e. the pure eigenstate corresponding to the largest eigenvalue of F.

3.4.1 Joint fidelity

In order to optimize the joint fidelity by the method sketched above, we need to determine the appropriate operator $F = F_{\mathrm{joint}}$. To this end, we calculate the joint fidelity from the characteristic functions of input and output states. By Eq. (3.18), the characteristic function of the output state $T_*(\rho)$ is $\chi_{\mathrm{out}}(\xi) = \chi_T(\Omega\,\xi)\,\chi_{\mathrm{in}}(\sum_i \xi_i)$. The reference state is the n-fold tensor product of the input state, described by $\prod_{i=1}^n \chi_{\mathrm{in}}(\xi_i) = \mathrm{tr}\big[\rho^{\otimes n}\,\mathrm{W}_{\xi_1,\ldots,\xi_n}\big]$. Together with the definition (3.1) and the non-commutative Parseval theorem (2.11), this yields:

$$\begin{aligned} f_{\mathrm{joint}}(T,\rho) &= \mathrm{tr}\big[T_*(\rho)\,\rho^{\otimes n}\big] \\ &= \int \frac{\mathrm{d}\xi}{(2\pi)^n}\;\chi_{\mathrm{out}}(\xi)\;\prod_{i=1}^n \chi_{\mathrm{in}}(\xi_i) \\ &= \int \frac{\mathrm{d}\xi}{(2\pi)^n}\;\chi_T(\Omega\,\xi)\;\chi_{\mathrm{in}}(\textstyle\sum_i \xi_i)\;\displaystyle\prod_{i=1}^n \chi_{\mathrm{in}}(\xi_i)\,. \end{aligned} \tag{3.24}$$

Since we can restrict the discussion to the vacuum as input state, we can fix its characteristic function as $\chi_{\mathrm{in}}(\xi) = \mathrm{tr}\big[|0\rangle\langle 0|\;\mathrm{W}_\xi\big] = \exp(-\xi^2/4)$, cf. Eq. (2.26). Grouping together the terms involving χ_{in}, substituting $\xi \mapsto \Omega^{-1}\,\xi$ and introducing a suitable quadratic form Γ, this can be rewritten as:

$$\begin{aligned} f_{\mathrm{joint}}(T) &= \frac{1}{n-1}\int \frac{\mathrm{d}\xi}{(2\pi)^n}\;\chi_T(\xi)\,\mathrm{e}^{-\xi^{\mathrm{T}}\cdot\Gamma\cdot\xi/4} \\ &= (n-1)^{-1}\;\mathrm{tr}[\rho_T\,F_{\mathrm{joint}}]\,, \end{aligned} \tag{3.25}$$

where we have again employed the Parseval relation (2.11) in the last line with characteristic functions $\chi_T(\xi)$ and $\exp(-\xi^{\mathrm{T}}\cdot\Gamma\cdot\xi/4)$ defining ρ_T and F_{joint}, respectively. For simplicity we have excluded the factor $|\det\Omega^{-1}| = (n-1)^{-1}$, cf. (3.21), from the definition of F_{joint}. Since the input state is fixed, the quadratic form Γ is determined solely by the linear transformation Ω from (3.19). As a consequence, the operator F_{joint} is independent from T, as required. Moreover, it is a Gaussian operator with covariance matrix Γ and in suitable canonical coordinates, it separates into a tensor product of single-mode thermal states. Maximizing the joint fidelity amounts to finding the maximal expectation value in Eq. (3.25). This is given by the largest

eigenvalue of F_{joint}, which in turn is the product of the largest eigenvalue of each of the thermal states in the tensor product and thus nondegenerate. It is attained for ρ_T as the unique eigenstate to the maximal eigenvalue, which is a suitably squeezed vacuum state. Hence the cloner optimal with respect to joint fidelity is Gaussian.

In order to determine these eigenvalues, we need the exact form of Γ and its symplectic eigenvalues. In (Q, P)-block representation and for coherent input states we get

$$\Gamma = (\Omega^{-1})^{\mathrm{T}} \cdot \begin{pmatrix} \mathbb{E}_n + \mathbb{1}_n & 0 \\ 0 & \mathbb{E}_n + \mathbb{1}_n \end{pmatrix} \cdot \Omega^{-1} = \begin{pmatrix} \frac{3-n}{(1-n)^2}\,\mathbb{E}_n + \mathbb{1}_n & 0 \\ 0 & \mathbb{E}_n + \mathbb{1}_n \end{pmatrix}$$

with Ω^{-1} from (3.22). To compute the symplectic eigenvalues of Γ, we turn back to the modewise representation and get

$$\Gamma = \mathbb{E}_n \otimes \begin{pmatrix} \frac{3-n}{(1-n)^2} & 0 \\ 0 & 1 \end{pmatrix} + \mathbb{1}_n \otimes \mathbb{1}_2\,, \tag{3.26}$$

where the indices of the square matrices indicate the dimension of the respective vector space. From the characteristic polynomial (3.20) of $\mathbb{E}_n$ it is clear that the spectrum of $\mathbb{E}_n$ consists of only n and 0 with multiplicities 1 and $n-1$, respectively. It follows that $\mathbb{E}_n$ can be diagonalized by an orthogonal transformation[5] Θ and that $(\Theta \otimes \mathbb{1}_2)^{\mathrm{T}} \cdot \Gamma \cdot (\Theta \otimes \mathbb{1}_2)$ is diagonal. Since in this modewise representation $\sigma = \mathbb{1}_n \otimes \sigma_{\text{in}}$, clearly $(\Theta \otimes \mathbb{1}_2)$ is a symplectic transformation. After squeezing by a factor of $(n-1)$ in one mode, the diagonal elements $(n+1)/(n-1)$ and 1 of Γ are its symplectic eigenvalues with multiplicities 1 and $n-1$, respectively. Hence F_{joint} can be decomposed into a tensor product of a one-mode thermal state with symplectic eigenvalue $(n+1)/(n-1)$ and $(n-1)$ modes of vacuum. Since by Eq. (2.33) the eigenvalues ν_j of a one-mode thermal state with covariance g are

$$\nu_j = \frac{2}{g+1}\left(\frac{g-1}{g+1}\right)^j,$$

we get for the largest eigenvalue of F_{joint} that $\max \operatorname{spec}(F_{\text{joint}}) = \nu_0 = (n-1)/n$ for $g = (n+1)/(n-1)$. By (3.25) this yields the desired maximal joint fidelity as

$$f_{\text{joint}} = \sup_T f_{\text{joint}}(T) = \max \operatorname{spec}(F_{\text{joint}})/(n-1) = \tfrac{1}{n}\,.$$

The optimal cloner can be described by a pure state ρ_T which in suitable coordinates corresponds to a tensor product of $n-1$ modes of unsqueezed vacuum and one mode of vacuum squeezed by a factor of $n-1$, i.e. it has a covariance matrix

$$\gamma_T = \begin{pmatrix} 1/(n-1) & 0 \\ 0 & n-1 \end{pmatrix} \oplus (\mathbb{1}_{n-1} \otimes \mathbb{1}_2)\,.$$

5 The eigenspace for the eigenvalue n is one-dimensional. In the subspace orthogonal to this eigenvector, choose an orthonormal basis. All its vectors will be eigenvectors to the eigenvalue 0. Together with the above eigenvector, they form a complete orthonormal basis in which $\mathbb{E}_n$ is diagonal.

Hence for the case $n = 2$ this is the cloner already known from [53, 54, 55]. Summarizing the results from above and Section 3.3.1 yields

Proposition 3.5:
The worst-case joint fidelity for 1-to-n cloning of coherent states is optimized by a permutation invariant Gaussian cloner covariant with respect to phase space displacements. The maximal fidelity is $1/n$.

The expression (3.24) for the joint fidelity reveals why the worst-case fidelity over *all* pure Gaussian states of any cloner is zero. Starting from a coherent state ρ, all pure Gaussian states can be obtained by applying a symplectic transformation $S \in \mathrm{Sp}(2, \mathbb{R})$ to each copy of ρ in the fidelity criterion, i.e. by replacing $\rho \mapsto U_S^* \, \rho \, U_S$. This corresponds to the substitution $\xi_i \mapsto S \cdot \xi_i$ in the argument of the input characteristic function $\chi_{\mathrm{in}}(\xi)$. Equivalently, in Eq. (3.25), the matrix Γ can be replaced by $\big(\bigoplus_{j=1}^n S^{\mathrm{T}}\big) \cdot \Gamma \cdot \big(\bigoplus_{j=1}^n S\big)$. For a single mode, any two phase space vectors ξ and η of finite length can be transformed into each other by a symplectic transformation S. To see this, refer to the Euler decomposition of S in Eq. (2.20): Choose an orthogonal transformation K' such that $K' \cdot \xi$ is parallel to $(1, 0)$, use the appropriate scaling r and another orthogonal transformation K such that $K^{\mathrm{T}} \eta$ is parallel to $(1, 0)$; then $\eta = S \cdot \xi$. Hence for any cloner given by a normal state with characteristic function χ_T, the exponential factor in the integrand of (3.25) can be twisted to maximal mismatch and be scaled by squeezing such that the fidelity is brought arbitrarily close to zero. The same arguments hold for the single-copy fidelity.

3.4.2 Single-copy fidelity

As in the case of joint fidelity, we determine the appropriate operators F_i from the output characteristic function in order to compute the single-copy fidelities as the expectation values of $\mathrm{tr}[\rho_T \sum_i \lambda_i \, F_i]$. By Eq. (3.18), the characteristic function of the i-th clone is given by $\chi_i(\xi_i) = \chi_{\mathrm{out}}(0, \ldots, 0, \xi_i, 0, \ldots, 0) = \mathrm{tr}[T(\rho) \; \mathrm{W}_{0,\ldots,0,\xi_i,0,\ldots,0}]$, where the zeros in the argument of the Weyl operator lead to tensor factors $\mathbb{1}$ and thus effectively trace out all clones except for the i-th. The fidelity of this clone is

$$f_i(T, \rho) = \int \frac{\mathrm{d}\xi_i}{2\pi} \; t(0, \ldots, 0, \xi_i, 0, \ldots, 0) \, \big(\chi_{\mathrm{in}}(\xi_i)\big)^2 . \tag{3.27}$$

In contrast to the reasoning for the joint fidelity, we will determine the operators F_i explicitly in terms of the field operators Q_j and P_j of each mode. To this end, we use $t(\xi) = \mathrm{tr}[\rho_T \; \mathrm{W}_{\Omega\,\xi}]$ from (3.17) and write the Weyl operator in the explicit form (2.6), $\mathrm{W}_{q_1,p_1,\ldots,q_n,p_n} = \exp\big(\mathrm{i} \sum_k (q_k \, P_k - p_k \, Q_k)\big)$. Together with (3.19) for Ω, this yields the Weyl operator in question as

$$\mathrm{W}_{\Omega\,(0,\ldots,0,q_i,p_i,0,\ldots,0)} = \exp\big(\mathrm{i} \, (p_i \, P_i - q_i \, \textstyle\sum_{i \neq j} Q_j)\big) \, .$$

Replacing $t(\xi)$ in (3.27) and letting $\xi_i = (q, p)$, the i-th single-copy fidelity for the fixed input state $|0\rangle\langle 0|$ is $f_i = \mathrm{tr}[\rho_T F_i]$, where

$$\begin{aligned} F_i &= \int \frac{\mathrm{d}q\,\mathrm{d}p}{2\pi} \left(\chi_{\mathrm{in}}(q,p)\right)^2 \exp\bigl(\mathrm{i}\,(p\,P_i - q\,\textstyle\sum_{i\neq j} Q_j)\bigr) \\ &= \exp\bigl(-P_i^2/2 - \textstyle\sum_{i\neq j} Q_j^2/2\bigr)\,. \end{aligned} \tag{3.28}$$

In the following, we study the weighted single-copy fidelities $\sum_i \lambda_i\, f_i$ by numerical computation and analytical arguments. For simplicity, we restrict this discussion to the case of 1-to-2 cloning. While in principle the method can be generalized, numerical computations of the fidelities might get more involved. The operator F for the weighted single-copy fidelity $\lambda\, f_1(T) + (1-\lambda)\, f_2(T) = \mathrm{tr}[\rho_T\, F]$ is composed of the weighted sum of the respective F_i:

$$F = \lambda_1\, \mathrm{e}^{-(Q_2^2+P_1^2)/2} + \lambda_2\, \mathrm{e}^{-(Q_1^2+P_2^2)/2} \tag{3.29a}$$

$$\simeq \lambda_1\, \mathrm{e}^{-(Q_1^2+Q_2^2)/2} + \lambda_2\, \mathrm{e}^{-(P_1^2+P_2^2)/2}\,, \tag{3.29b}$$

where the second expression is obtained by applying an orthogonal, symplectic transformation such that $Q_1 \mapsto -P_1$ and $P_1 \mapsto Q_1$. Both forms are equivalent for the purpose of computing eigenvalues. The largest eigenvalue of F gives the maximal single-copy fidelity, the corresponding eigenvector describes the optimal cloner. Before we detail their approximate computation, we discuss the results depicted in Fig. 3.2.

Since a linear combination of Gaussian operators as in (3.29b) does in general not have Gaussian eigenfunctions, the optimal cloners are not Gaussian. In fact, comparing the optimal symmetric cloner yielding $f_1 = f_2 \approx 0.6826$ with the best Gaussian cloner (see [53,54,55] and below), limited to $f_1 = f_2 = \frac{2}{3}$, already indicates the enhancement in fidelity by non-Gaussian cloners. A more detailed study of the best Gaussian 1-to-2 cloners (see below) results in the dotted curve of fidelity pairs in Fig. 3.2. Clearly, the non-Gaussian cloners perform better for every region of the diagram. The two symmetric cloners can be found at the intersection of the dash-dotted diagonal with the dotted curve of best Gaussian cloners and the solid curve of optimal cloners. At the points of the singular cloners with $f_1, f_2 = 1$, the solid curve of optimal cloners has a nonfinite slope $s = \infty$ and $s = 0$, respectively, while the dotted curve of the best Gaussian cloners has a finite slope (see in particular (b) in Fig. 3.2). By the arguments of Section 3.2, this implies that the optimal cloners for $f_1 \neq 1$, $f_2 \neq 1$ do not coincide with the singular cloners. In contrast, the best Gaussian cloners for $f_1 \approx 1$ and $f_2 \approx 1$ are determined by the respective singular cloners; see also below. The trivial »copy-through« cloners, which yield fidelity $f_1 = 1$ or $f_2 = 1$, are singular in any case by Corollary 3.3.

The following subsection gives details on the approximate, numerical computation of the largest eigenvalue of F and the corresponding eigenfunctions. To complement the results on optimal cloners, the last two subsections briefly investigate the best Gaussian cloner for 1-to-2 cloning with arbitrary weights and for symmetric 1-to-n cloning. Before this, we summarize the results in

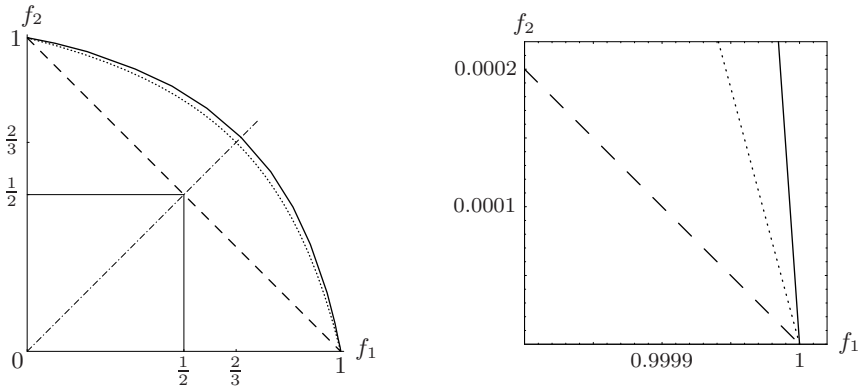


Figure 3.2:
Achievable pairs (f_1, f_2) of single-copy fidelities in 1-to-2 cloning of coherent states. The dots represent the optimal Gaussian cloner, while the solid curve indicates optimal non-Gaussian operations. Fidelities in the lower left quadrant are accessible to measure-and-prepare schemes (cf. Section 3.4.3). Classical mixtures of the two »trivial« cloners fall onto the dashed line. The dash-dotted diagonal marks symmetric cloners, with intersection points corresponding to the best classical, best Gaussian, and optimal cloning, respectively. The inset shows the infinite slope at $f_1 = 1$ for non-Gaussian cloners as opposed to the Gaussian case. For a schematic version of this graph and further explanations see Fig. 3.1 and Section 3.2.

Proposition 3.6:
The weighted single-copy fidelities for 1-to-n cloning of coherent states are optimized by non-Gaussian cloners. For 1-to-2 cloning, the optimal symmetric cloner yields fidelities $f_{1,2} \approx 0.6826$. The optimal cloners are nonsingular except for the cases $f_{1,2} = 1$. The best Gaussian 1-to-2 cloners are described by rotation invariant, squeezed Gaussian wave functions. They are nonsingular for weight $\frac{1}{5} < \lambda < \frac{4}{5}$ and correspond to the singular cloners beyond this regime. In the symmetric case $\lambda = \frac{1}{2}$, the fidelities are $f_{1,2} = \frac{2}{3}$. The best symmetric Gaussian 1-to-n cloners yield fidelities $f_i = (2 - 1/n)^{-1}$.

Numerical optimization

In order to approximately calculate the largest eigenvalue of F in (3.29b), we numerically compute the expectation value $\langle\phi_n|\, F\, |\phi_n\rangle$ of F in a state obtained from the iteration $\phi_{n+1} = F\,\phi_n / \|F\,\phi_n\|$. This power iteration effectively suppresses the parts of ϕ_0 outside the eigenspace to the largest eigenvalue, so $\langle\phi_n|\, F\, |\phi_n\rangle$ approximates the largest eigenvalue of F. From the resulting function ϕ_n, the single-copy fidelities can be computed as the expectation values of the constituents of F, $f_1 = \langle\phi_n|\, \mathrm{e}^{-(Q_1^2+Q_2^2)/2}\, |\phi_n\rangle$ and $f_2 = \langle\phi_n|\, \mathrm{e}^{-(P_1^2+P_2^2)/2}\, |\phi_n\rangle$. Varying the weight λ yields the points on the solid curve in Fig. 3.2.

The starting point for the power iteration is a rotation invariant Gaussian function $\phi_c(x, y) \propto \exp(-c\,(x^2 + y^2))$. The squeezing value c is taken from the optimal Gaussian cloner where available, i.e. for $0.2 < \lambda < 0.8$ (see the discussion of optimal Gaussian 1-to-2 cloners below). Samples for the solid curve in Fig. 3.2 from this regime are taken in the interval $0.25 \leq \lambda \leq 0.75$ with increment 0.05 and an iteration depth of eight steps. Alternatively, we start from the state ϕ_c resulting from the iteration for $\lambda = 0.79$ with nine steps and scale the squeezing parameter c by a heuristically determined factor of $(-\log l)^9$. Sampling the parameter l for $0.24 \leq l \leq 0.36$ and $0.64 \leq l \leq 0.76$ with increment 0.02 yields further points on the outskirts of the curve. The fidelity pairs obtained by this method are well separated from the points representing the singular cloners and the iteration does not tend towards a singular state. Moreover, the eigenstate to the largest eigenvector is a pure state with wave function $\phi(x)$. It is unique by the following argument: Both operators $\exp\bigl(-(Q_1^2 + Q_2^2)/2\bigr)$ and $\exp\bigl(-(P_1^2 + P_2^2)/2\bigr)$ correspond to positive integral kernels, hence replacing any wave function $\psi(x)$ by $|\psi(x)|$ yields larger expectation values while preserving the norm. Assume two states $\psi_1(x) \geq 0$ and $\psi_2(x) \geq 0$ were both eigenstates to the largest eigenvalue. Then so is any linear combination $p_1\,\psi_1(x) - p_2\,\psi_2(x)$. However, since $|p_1\,\psi_1(x) - p_2\,\psi_2(x)|$ yields larger expectation values, the conclusion is $\psi_1(x) \equiv \psi_2(x)$ and the eigenstate to the largest eigenvector is unique.

Addendum: On suggestion of a referee, we complement this discussion with more details. Note that the following paragraphs have been added after acceptance of the thesis.

All expressions arising in the iteration $\phi_{n+1} = F\,\phi_n / \|F\,\phi_n\|$ have been ob-

tained without approximations. Since the initial function ϕ_0 is chosen as a Gaussian, the action of F on ϕ_n yields again Gaussian functions and the scalar products $f_1 = \langle\phi_n|\,\mathrm{e}^{-(Q_1^2+Q_2^2)/2}\,|\phi_n\rangle$ and $f_2 = \langle\phi_n|\,\mathrm{e}^{-(P_1^2+P_2^2)/2}\,|\phi_n\rangle$ decompose into sums of Gaussian integrals, which can be evaluated analytically.

As has been argued above, the highest eigenvalue of F cannot be degenerated. Hence the speed of convergence of $\langle\phi_n|\,F\,|\phi_n\rangle$ towards the largest eigenvalue of F can be determined from the distances $\Delta_n = \|\phi_n - \phi_{n-1}\|$. Since the distances Δ_n decrease exponentially, the gain of accuracy by further iteration can be estimated from the slope of $\log\Delta_n$.

The spectrum of the fidelity operator F can be investigated in more detail by splitting off the compact contributions. Consider F and F^2,

$$\begin{aligned} F &= \lambda\,\mathrm{e}^{-(Q_1^2+Q_2^2)/2} + (1-\lambda)\,\mathrm{e}^{-(P_1^2+P_2^2)/2}\,, \\ F^2 &= \lambda^2\,\mathrm{e}^{-(Q_1^2+Q_2^2)} + (1-\lambda)^2\,\mathrm{e}^{-(P_1^2+P_2^2)} + \text{compact part}\,, \end{aligned}$$

where the compact part of F^2 contains contributions of the form $\mathrm{e}^{-Q^2}\,\mathrm{e}^{-P^2}$ and $\mathrm{e}^{-P^2}\,\mathrm{e}^{-Q^2}$. The compact part can be eliminated by identifying all compact operators with zero or, formally, by dividing the initial algebra into equivalence classes whose elements differ only by a compact operator.[6] Then F^2 is identified with an operator K as

$$F^2 \simeq K \equiv \lambda^2\,\mathrm{e}^{-(Q_1^2+Q_2^2)} + (1-\lambda)^2\,\mathrm{e}^{-(P_1^2+P_2^2)}\,.$$

With a parameter z which obeys

$$\max\{\lambda, 1-\lambda\} \le z \le 1$$

and the relations

$$\begin{aligned} 0 \le \mathrm{e}^{-(Q_1^2+Q_2^2)} &\le \mathrm{e}^{-(Q_1^2+Q_2^2)/2} \le \mathbb{1}\,, \\ 0 \le \mathrm{e}^{-(P_1^2+P_2^2)} &\le \mathrm{e}^{-(P_1^2+P_2^2)/2} \le \mathbb{1}\,, \end{aligned}$$

we can estimate

$$\begin{aligned} K &= \lambda^2\,\mathrm{e}^{-(Q_1^2+Q_2^2)} + (1-\lambda)^2\,\mathrm{e}^{-(P_1^2+P_2^2)} \\ &\le z\,\lambda\,\mathrm{e}^{-(Q_1^2+Q_2^2)/2} + z\,(1-\lambda)\,\mathrm{e}^{-(P_1^2+P_2^2)/2} = z\,F\,. \end{aligned}$$

This implies that the noncompact parts of F^2 and F obey $F^2 \le z\,F$ and hence the essential spectrum of F lies below $\max\{\lambda, 1-\lambda\}$. In reverse, the spectrum above $\max\{\lambda, 1-\lambda\}$ consists of discrete eigenvalues of finite multiplicity. In particular, this applies to the maximal eigenvalue of F, which guarantees the functioning of the power iteration. ◊

6 This is equivalent to considering F^2 in the Calkin algebra.

The power iteration described above does not work well in the vicinity of the trivial cloners with $f_1 = 1$ or $f_2 = 1$. Instead, we use a different family of non-Gaussian, highly squeezed states ϕ_c and directly evaluate $\langle\phi_c|\, F\, |\phi_c\rangle$, varying the squeezing parameter c. These states are described by $\phi_c(x_1, x_2) = c\,\phi(c\,x_1, c\,x_2)$ in a representation on $\mathcal{L}^2(\mathbb{R}^2, \mathrm{d}x_1\,\mathrm{d}x_2)$, such that $\|\phi_c\|_2 = \|\phi\|_2$. In momentum space $\mathcal{L}^2(\mathbb{R}^2, \mathrm{d}p_1\,\mathrm{d}p_2)$, they are represented by the Fourier transformed function $\hat{\phi}_c(p_1, p_2) = \hat{\phi}(p_1/c, p_2/c)/c$. According to Eq. (3.29b), the single-copy fidelities for a cloner determined by these states in the limit $c \to \infty$ are

$$\begin{aligned} f_1(c) &= \langle\phi_c|\, \mathrm{e}^{-(Q_1^2+Q_2^2)/2}\, |\phi_c\rangle \\ &= \int \mathrm{d}x_1 \mathrm{d}x_2\; |\phi(x_1, x_2)|^2\, \mathrm{e}^{-(x_1^2+x_2^2)/(2c^2)} \\ &\to 1 - \frac{1}{2c^2} \int \mathrm{d}x_1 \mathrm{d}x_2\; |\phi(x_1, x_2)|^2\, (x_1^2 + x_2^2)\,, \end{aligned} \tag{3.30a}$$

$$\begin{aligned} f_2(c) &= \langle\hat{\phi}_c|\, \mathrm{e}^{-(P_1^2+P_2^2)/2}\, |\hat{\phi}_c\rangle \\ &= \int \mathrm{d}p_1 \mathrm{d}p_2\; |\hat{\phi}(p_1, p_2)|^2\, \mathrm{e}^{-(p_1^2+p_2^2)c^2/2} \\ &= \frac{2\pi}{c^2} \int \mathrm{d}p_1 \mathrm{d}p_2\; |\hat{\phi}(p_1, p_2)|^2\, \frac{c^2}{2\pi}\, \mathrm{e}^{-(p_1^2+p_2^2)c^2/2} \\ &\to \frac{2\pi}{c^2} |\hat{\phi}(0, 0)|^2\,. \end{aligned} \tag{3.30b}$$

This case describes the cloner in the vicinity of $f_1 = 1$. Differentiating both quantities with respect to c^2 yields the slope $s = \mathrm{d}f_2/\mathrm{d}f_1 = f_2/(f_1 - 1)$. In order to show that s approaches $-\infty$, we choose the family of functions generated by $\phi(x_1, x_2) = 1/(\epsilon + x_1^2 + x_2^2)$. Introducing polar coordinates, we approximately evaluate the relevant quantities in (3.30) as

$$\begin{aligned} \int \mathrm{d}x_1 \mathrm{d}x_2\; |\phi(x_1, x_2)|^2\, (x_1^2 + x_2^2) &\approx 2\pi \int_0^R \mathrm{d}r\; r^3\, \frac{1}{(\epsilon + r^2)^2} \\ &= \pi \int_\epsilon^{\epsilon+R^2} \mathrm{d}t\; (t - \epsilon)\, \frac{1}{t^2} \\ &= \pi\, \log \frac{\epsilon + R^2}{\epsilon} + \pi \left(\frac{\epsilon}{\epsilon + R^2} - 1 \right), \\ 2\pi\, \hat{\phi}(0, 0) &= \int \mathrm{d}x_1 \mathrm{d}x_2\; \phi(x_1, x_2) \\ &\approx 2\pi \int_0^R \mathrm{d}r\; \frac{r}{\epsilon + r^2} \end{aligned}$$

$$= \pi \int_0^{R^2} \frac{\mathrm{d}t}{\epsilon + t} = \pi \, \log \frac{\epsilon + R^2}{\epsilon} \,,$$

where the approximations become exact for $R \to \infty$. Using these expressions to compute the slope yields $s \to -\infty$ for $R \to \infty$ and arbitrary ϵ, c. By the argument in Section 3.2, this implies that the optimal cloners in the vicinity of $f_1 = 1$ do not become singular. Since the problem is symmetric with respect to interchange of f_1 and f_2, the result can be shown to also hold for $f_2 = 1$ by exchanging the squeezing parameter c for $1/c$.

The solid curve in Fig. 3.2 was complemented with fidelity pairs (f_1, f_2) from the above expressions sampled at $R = 1000, \epsilon = \mathrm{e}^l, c = 100\, l^{-4}$ for $0.1 \leq l \leq 0.9$ and $0.6 \leq l \leq 1.4$ with increments of 0.1.

Best Gaussian 1-to-2 cloners

The best Gaussian cloners for a given weighted single-copy fidelity $\lambda f_1 + (1 - \lambda) f_2$ maximize the expectation value of F in (3.29b) with respect to Gaussian states ρ_T. Since F is invariant under simultaneous rotation of the Q_i and P_i, an averaging argument similar[7] to that in Section 3.3 implies that the maximizing states ρ_T are also rotation invariant and thus are described by a rotation invariant Gaussian function $\phi_c(x_1, x_2) \propto \exp\bigl(-c\,(x_1^2 + x_2^2)\bigr)$ for $\rho_T = |\phi_c\rangle\langle\phi_c|$ in the $\mathcal{L}^2(\mathbb{R}^2, \mathrm{d}x_1\, \mathrm{d}x_2)$ representation. Depending on the squeezing parameter c, these cloners yield fidelities $(f_1, f_2) = \bigl(2/(2 + c^{-1}), 2/(2 + c)\bigr)$. The squeezing c_{opt} which yields an optimal weighted fidelity $\lambda\, f_1 + (1 - \lambda)\, f_2$ can be calculated analytically from the weight λ,

$$c_{\mathrm{opt}} = \frac{2 - 4\,\lambda + 3\,\sqrt{\lambda\,(1 - \lambda)}}{5\,\lambda - 1} \quad \text{for } \tfrac{1}{5} < \lambda < \tfrac{4}{5}\,.$$

The resulting fidelities are plotted as the dotted curve in Fig. 3.2. At the intersection with the dash-dotted diagonal lies the best Gaussian symmetric cloner with $\lambda = \frac{1}{2}$, fidelities $f_1 = f_2 = \frac{2}{3}$ and squeezing $c = 1$. This is the cloner already known from [53, 54, 55] (see also its optical implementation in Section 3.5, where the state ϕ_c is explicitly used as the idler mode of an OPA).

In the regimes of $\lambda \geq \frac{1}{5}$ and $\lambda \leq \frac{4}{5}$, the above expression yields values $c_{\mathrm{opt}} = \infty$ and $c_{\mathrm{opt}} = 0$, respectively. The corresponding cloners are no longer described by a density matrix $\rho_T = |\phi_c\rangle\langle\phi_c|$, but by singular, »infinitely squeezed« states [44]. This implies that for strongly asymmetric single-copy fidelities with $\lambda \leq \frac{1}{5}$ or $(1 - \lambda) \leq \frac{1}{5}$, the singular cloners mapping the input state exactly into one of the output systems are optimal. Geometrically, this result corresponds to a finite slope of the dotted curve in Fig. 3.2 at the end points. The discussion in Section 3.2 connects this slope to the weight λ_0 up to which the singular cloners are optimal. From $\lambda_0 = \frac{1}{5}$ in this case, the slope computes to $s = -\frac{1}{4}$.

7 However, since the symmetry group in this case is compact, the averaging does not have to resort to an invariant mean but can use the Haar measure of the group.

Best symmetric Gaussian 1-to-n cloners

By a symmetric Gaussian cloner we understand a cloning map which is invariant under interchanging the output modes and which is described by a Gaussian state ρ_T. To investigate these cloners, we use the characteristic function t with respect to the twisted symplectic form $\Sigma = (\mathbb{1}_n - \mathbb{E}_n) \otimes \sigma_{\text{in}}$, confer Eq. (3.16) and its discussion in Section 3.3.2.

For the cloner to be symmetric and Gaussian, t has to have the form

$$t(\xi) = \exp\bigl(-\xi^{\text{T}} \cdot (a\,\mathbb{1}_n \otimes \mathbb{1}_2 + b\,\mathbb{E}_n \otimes \mathbb{1}_2) \cdot \xi/4\bigr)\,. \tag{3.31}$$

The map is completely positive if an only if $(a\,\mathbb{1}_n \otimes \mathbb{1}_2 + b\,\mathbb{E}_n \otimes \mathbb{1}_2) - \mathrm{i}\Sigma \geq 0$. Introducing the abbreviations

$$A = a\,\mathbb{1}_2 - \mathrm{i}\sigma_{\text{in}}\,,\ B = b\,\mathbb{1}_2 + \mathrm{i}\sigma_{\text{in}} \text{ and } X = \mathbb{1}_n \otimes A + \mathbb{E}_n \otimes B\,, \tag{3.32}$$

this condition is equivalent to $X \geq 0$, which in turn is true if and only if $\langle\phi|\,X\,|\phi\rangle \geq 0$ for all $\phi = \bigoplus_{j=1}^n \phi_j$, $\phi_j \in \mathbb{C}^2$. The evaluation of this condition is simplified by rewriting $\phi_j = \psi_j + \psi_0$ where $\psi_0 = \sum_j \phi_j/n$ and hence $\sum_j \psi_j = 0$:

$$\begin{aligned}\langle\phi|\,X\,|\phi\rangle &= \sum_{j=1}^n \langle\phi_j|\,A\,|\phi_j\rangle + \sum_{i,j=1}^n \langle\phi_j|\,B\,|\phi_i\rangle \\ &= \sum_{j=1}^n \langle\psi_j|\,A\,|\psi_j\rangle + n\,\langle\psi_0|\,A\,|\psi_0\rangle + n^2\,\langle\psi_0|\,B\,|\psi_0\rangle\,.\end{aligned}$$

By evaluating this expression for particular ψ_j it is easily seen that $A \geq 0$ and $n\,B + A \geq 0$ are necessary and sufficient conditions for $X \geq 0$:

$$\begin{aligned}\psi_1 = -\psi_2 \neq 0\,,\ \psi_{i\neq 1,2} = 0 \quad &\Rightarrow \quad \langle\phi|\,X\,|\phi\rangle = 2\,\langle\psi_1|\,A\,|\psi_1\rangle\,, \\ \psi_0 \neq 0\,,\ \psi_{i\neq 0} = 0 \quad &\Rightarrow \quad \langle\phi|\,X\,|\phi\rangle = n\,\langle\psi_0|\,A\,|\psi_0\rangle + n^2\,\langle\psi_0|\,B\,|\psi_0\rangle\,.\end{aligned}$$

The definitions in (3.32) imply that the above conditions on A and B are variants of the state conditions on covariance matrices (2.22) which are fulfilled if and only if $a \geq 1$ and $a + n\,b \geq n - 1$.

Since the cloner is symmetric with respect to interchanging the output modes, all single-copy fidelities are identical. They are calculated as the overlap between one output subsystem, e.g. the first, and the fixed input state $|0\rangle\langle 0|$ with characteristic function $\chi_{\text{in}}(\xi) = \exp(-\xi^2/4)$:

$$\begin{aligned}f_{\text{symmetric}}(T) = f_1\bigl(T, |0\rangle\langle 0|\bigr) &= \operatorname{tr}\bigl[T\bigl(|0\rangle\langle 0| \otimes \mathbb{1} \otimes \ldots \otimes \mathbb{1}\bigr)\,|0\rangle\langle 0|\bigr] \\ &= \int \frac{\mathrm{d}\xi}{2\pi}\, t(\xi, 0, \ldots, 0)\,\bigl(\chi_{\text{in}}(\xi)\bigr)^2 \\ &= \int \frac{\mathrm{d}\xi}{2\pi}\, \mathrm{e}^{-(a+b+2)\,\xi^2/4} = \frac{2}{a+b+2} \qquad (3.33a) \\ &\leq \frac{n}{2n-1} \to \frac{1}{2} \quad \text{for } n \to \infty\,, \qquad (3.33b)\end{aligned}$$

where the bound is imposed by the state conditions above and is reached for $a = 1$ and $b = (n-1-a)/n$. As is to be expected, this cloner performs better than the best classical cloner (cf. Section 3.4.3) for any finite number n of clones, but approaches the classical limit for $n \to \infty$. The classical case can be exactly implemented by letting $a = 1$ and $b = 1$, which is the lowest value for b independent of n. By (3.33a), this yields $f_{\text{symmetric}} = \frac{1}{2}$. For the case $n = 2$, we recover from (3.33b) the fidelities $f_1 = f_2 = f_{\text{symmetric}} = \frac{2}{3}$ from the discussion of the best Gaussian 1-to-2 cloners above and from [53, 54, 55]. In fact, the best symmetric Gaussian 1-to-n cloner is described by the same state as the optimal joint fidelity cloner (see Section 3.4.1), as can be seen by a transformation of the covariance matrix from $t(\xi)$ in (3.31) for the optimal a and b with Ω^{-1} from (3.22).

3.4.3 Classical cloning

The methods described in the previous sections can also be used to investigate the cloning of coherent states by classical means, i.e. a protocol that relies on classical information without any additional quantum resource (e.g. shared entanglement) to produce output states which resemble the quantum input states. An example is a measure-and-prepare scheme which employs the classical information obtained by a measurement on the input to prepare an unlimited number of output systems in an identical quantum state [64, 65]. Although classical schemes are potential 1-to-∞ cloning maps, we describe them as »1-to-1« cloners, $T\colon \operatorname{ccr}(\Xi, \sigma_{\text{in}}) \to \operatorname{ccr}(\Xi, \sigma_{\text{in}})$, and assume that the classical information can be stored and reused to prepare an arbitrary number of output systems in the same state. This is indeed true for the optimal cloner, see below. The result justifies the restriction to 1-to-1 cloners, because preparing n clones (classically) from the same input cannot yield a higher fidelity for any of the clones. Note that classical 1-to-1 cloning is nothing but classical teleportation, i.e. the transmission of quantum information over a classical channel without supplemental entanglement; cf. Section 3.6.

By the arguments in Section 3.3, T is covariant and thus maps Weyl operators to multiples of Weyl operators, $T(\mathrm{W}_\xi) = t(\xi)\ \mathrm{W}_\xi$, according to Section 3.3.2. This definition does, however, not include the restriction that T is a classical operation. Especially, $t(\xi)$ is the characteristic function of a state on a *classical*, i.e. commutative algebra and can be chosen as $t \equiv 1$, which leads to the trivial cloner $T = \mathrm{id}$. But since T corresponds to a classical operation, it has to be completely positive if composed with time reversal[8] τ. Letting $\xi = (q, p)$, this combined map is defined on Weyl operators by

$$(\tau \circ T)(\mathrm{W}_{q,p}) = t(q, p)\ \mathrm{W}_{q,-p}\,,$$

where t is the characteristic function of a state on $\operatorname{ccr}(\Xi, \Sigma)$ for $\Sigma(\xi, \eta) = 2\,\sigma_{\text{in}}(\xi, \eta) = \sigma_{\text{in}}(\Omega\,\xi, \Omega\,\eta)$ with $\mathbb{R} \ni \Omega = \sqrt{2}$. Hence $t(\xi) = \chi_T(\sqrt{2}\,\xi)$, where $\chi_T(\xi)$ is the characteristic function of a state on $\operatorname{ccr}(\Xi, \sigma)$. Using the form (3.18) for the output character-

8 This implies that the map $T \otimes \mathrm{id}$ is positive under partial transposition in the first tensor factor. Applying such channels T destroys any entanglement in the input state except for PPT-bound entanglement.

istic function, $\chi_{\rm out}(\xi_1,\ldots,\xi_n) = \chi_T(\Omega\,\xi)\,\chi_{\rm in}(\sum_i \xi_i)$, we can compute the fidelity of such cloners. Since there is only one output subsystem, the distinction between single-copy and joint fidelity is not necessary and we write $f_{\rm classical}(T) = f_{\rm joint}(T) = f_i(T)$. For covariant T, we can evaluate the fidelity for the fixed input state $|0\rangle\langle 0|$:

$$\begin{aligned} f_{\rm classical}(T) &= f_{\rm classical}\big(T, |0\rangle\langle 0|\big) = {\rm tr}\big[T\big(|0\rangle\langle 0|\big)\,|0\rangle\langle 0|\big] \\ &= \int \frac{{\rm d}\xi}{2\pi}\,\chi_T\big(\sqrt{2}\xi\big)\,\big(\chi_{\rm in}(\xi)\big)^2 = \frac{1}{2}\int \frac{{\rm d}\xi}{2\pi}\,\chi_T(\xi)\,\chi_{\rm in}(\xi) \\ &= \tfrac{1}{2}\,{\rm tr}\big[\rho_T\,|0\rangle\langle 0|\big] \le \tfrac{1}{2}\,, \end{aligned} \tag{3.34}$$

where $\chi_{\rm in}(\xi) = \exp(-\xi^2/4)$ is the characteristic function of the input state $|0\rangle\langle 0|$. This bound is tight, which has been proven in [63]. However, for completeness and further investigation we provide

Lemma 3.7:
The fidelity bound (3.34), $f_{\rm classical}(T) \le \frac{1}{2}$, can be reached by a heterodyne measurement and preparation of coherent states according to the measurement result. Moreover, this scheme can be extended to a 1-to-n cloner which yields the same fidelity and is Gaussian as well as covariant.

Proof: A heterodyne measurement is modeled as a POVM[9] $\big\{|\mu\rangle\langle\mu|/(2\pi)\big\}$ based on coherent states $\mu \in \mathcal{S}\big({\rm ccr}(\Xi_{\rm in},\sigma_{\rm in})\big)$. The probability $p_\alpha(\mu)$ of finding the measurement outcome μ for a coherent input state $\alpha \in \mathcal{S}\big({\rm ccr}(\Xi_{\rm in},\sigma_{\rm in})\big)$ is

$$\begin{aligned} p_\alpha(\mu) &= {\rm tr}\big[|\alpha\rangle\langle\alpha|\,|\mu\rangle\langle\mu|/(2\pi)\big] = \frac{1}{2\pi}\int \frac{{\rm d}\xi}{2\pi}\,\overline{\chi_\alpha(\xi)}\,\chi_\mu(\xi) \\ &= \frac{1}{2\pi}\int \frac{{\rm d}\xi}{2\pi}\,\exp\big(-\xi^2/2 + {\rm i}\xi^{\rm T}\cdot(\mu-\alpha)\big) = {\rm e}^{-(\mu-\alpha)^2/2}/(2\pi)\,, \end{aligned}$$

where $\chi_\alpha(\xi) = \exp(-\xi^2/2 + {\rm i}\xi^{\rm T}\cdot\alpha)$ is the characteristic function of the coherent state α (likewise for μ) and the bar denotes complex conjugation. In order to produce n clones of the input state, the output $\rho_{\rm out}$ is a classical mixture of n-fold tensor products $|\mu\rangle\langle\mu|^{\otimes n}$ of coherent states μ, weighted with the probabilities $p_\alpha(\mu)$:

$$\rho_{\rm out} = \int {\rm d}\mu\, p_\alpha(\mu)\,|\mu\rangle\langle\mu|^{\otimes n},$$

resulting in a characteristic function

$$\begin{aligned} \chi_{\rm out}(\xi) &= {\rm tr}\big[\rho_{\rm out}\,{\rm W}_\xi\big] = \int {\rm d}\mu\; p_\alpha(\mu)\;{\rm tr}\big[|\mu\rangle\langle\mu|^{\otimes n}\,{\rm W}_\xi\big] \\ &= \frac{1}{2\pi}\int {\rm d}\mu\;\exp\big(-(\mu-\alpha)^2/2 - \xi^2/4 + {\rm i}\textstyle\sum_{j=1}^n \xi_j^{\rm T}\cdot\mu\big) \\ &= \exp\big(-\xi^2/4 + (\textstyle\sum_{j=1}^n \xi_j)^2/2 + {\rm i}\sum_{j=1}^n \xi_j^{\rm T}\cdot\alpha\big) \\ &= \exp\big(-\xi^{\rm T}\cdot(\mathbb{1}_n\otimes\mathbb{1}_2 + 2\,\mathbb{E}_n\otimes\mathbb{1}_2)\cdot\xi/4 + {\rm i}\textstyle\sum_{j=1}^n \xi_j^{\rm T}\cdot\alpha\big)\,, \end{aligned} \tag{3.35}$$

9 A positive-operator-valued measurement (POVM) [1], also called generalized measurement, is a discrete or continuous set of positive operators $\{M_j\}$ which resolve unity, i.e. $\int {\rm d}j\; M_j = \mathbb{1}$ where the symbol $\int {\rm d}j$ denotes a discrete summation or a continuous integration.

where $\mathbb{E}_n$ is the matrix fully occupied with 1, defined for Eq. (3.19). Decomposing χ_{out} into the input part χ_{in} and the channel part t according to Eq. (3.16) yields $t(\xi) = \exp\bigl(-\xi^{\text{T}} \cdot (\mathbb{1}_n \otimes \mathbb{1}_2 + \mathbb{E}_n \otimes \mathbb{1}_2) \cdot \xi/4\bigr)$. This is the characteristic function (3.31) of the best symmetric Gaussian 1-to-n cloner considered in Section 3.4.2 for the classical case, i.e. for $a = b = 1$. This cloner indeed yields equal single-copy fidelities of $f_i = \frac{1}{2}$, cf. Eq. (3.33a). It is covariant by design, cf. Section 3.3.2, and also manifestly, because the output state inherits the displacement vector α from the input state, see (3.35). □

Remark: For a single clone, e.g. the first one, the output characteristic function $\chi_{\text{out}}(\xi_1, 0, \ldots, 0) = \exp\bigl(-\xi_1^2/4 + \xi_1^2/2 + \mathrm{i}\xi_1^{\text{T}} \cdot \alpha\bigr)$ corresponds to the input coherent state $|\alpha\rangle\langle\alpha|$ plus two units of vacuum noise.

The characterization of classical 1-to-1 cloners or classical teleportation by time reversal extends to cloners which are supplemented by PPT-bound entangled states [45]:

Lemma 3.8:
Every classical teleportation protocol assisted by a PPT-bound entangled state ω corresponds to a channel T which is completely positive under transposition of the input density operator in the Schrödinger picture. That is, if Θ denotes matrix transposition, then $T_* \circ \Theta$ is completely positive.

Remark: Note that in Schrödinger representation, time reversal of observables corresponds to transposition of the Hermitian density operator, cf. [15].

Proof: Denote the Hilbert space of the input state ρ by $\mathcal{H}_I$ and the Hilbert space of the bipartite, PPT-entangled state ω by $\mathcal{H}_A \otimes \mathcal{H}_B$. Since the teleportation protocol is classical, the corresponding channel T_* in the Schrödinger picture can be represented by a set of Kraus operators $\{M_i \otimes R_i\}$ in product form, cf. Section 2.3. The operators M_i act on the input plus one part of the entangled state, i.e. on $\mathcal{H}_I \otimes \mathcal{H}_A$, and play the role of the »measurement«. The R_i act on $\mathcal{H}_B$ and turn the second part of ω into the desired output state, thus corresponding to the »repreparation«. Hence T_* is represented as

$$T_*(\rho) = \sum_i \mathrm{tr}_{I,A}\bigl[(M_i \otimes R_i)\,(\rho \otimes \omega)\,(M_i \otimes R_i)^*\bigr]\,,$$

where $\mathrm{tr}_{I,A}$ denotes the partial trace over subsystems I and A. Since the trace is invariant under transposition of its argument, we can transpose the above expression with respect to systems I and A to obtain for $T_* \circ \Theta$:

$$(T_* \circ \Theta)(\rho) = T_*(\rho^{\text{T}}) = \sum_i \mathrm{tr}_{I,A}\bigl[(\overline{M}_i \otimes R_i)\,(\rho \otimes \omega^{\text{T}_A})\,(\overline{M}_i \otimes R_i)^*\bigr]\,,$$

where ω^{T_A} denotes the partial transposition of ω with respect to system A. If ω has positive partial transpose, i.e. if $\omega^{\text{T}_A} \geq 0$, then $T_* \circ \Theta$ is completely positive, since it is implemented by a set of Kraus operators $\{\overline{M}_i \otimes R_i\}$. □

By virtue of this lemma, the fidelity bound for classical cloning also applies to cloners which are not purely classical but make use of supplemental PPT-bound entangled states to link measurement and preparation. However, assisting the process with non-PPT entanglement can result in substantially higher fidelities, as this operation describes the teleportation of coherent states [58, 59]. Our derivation of the limit (3.34) thus proves and extends a success criterion for continuous-variable teleportation [63, 64], cf. Section 3.6. As the result of this section, we obtain

Proposition 3.9:
Classical cloning of coherent states realized by measuring the input state and repreparing output states depending on the results is limited to fidelities $f \leq \frac{1}{2}$. Supplemental PPT-bound entangled states do not improve this limit. The optimal cloner is Gaussian and covariant.

For the case of an unassisted measure-and-prepare scheme, an independent proof has been given in [46]. In Fig. 3.2, the achievable fidelities for classical cloners lie in the lower left quadrant with $f_1 \leq \frac{1}{2}$ and $f_2 \leq \frac{1}{2}$.

3.4.4 Bosonic output

Symmetric cloners yield the same single-copy fidelity for each clone. It is an obvious question if this implies further symmetries for the output state of the cloner. In particular, the output might lie in the bosonic sector, i.e. be invariant under the interchange of two clones. Note that this is not necessarily true since different states for individual clones could lead to the same single-copy fidelity. We show below that the output of symmetric covariant cloners belongs to the bosonic sector if the cloner is described by a bosonic state. Moreover, this condition is met by all *optimal* symmetric cloners considered in this chapter (cf. Proposition 3.11 below).

To formalize the statement, we introduce the flip operator $\mathbb{F}^{(i,j)}$ which acts on vectors $|\psi\rangle \in \mathcal{H}^{\otimes n}$ by interchanging tensor factors i and j:

$$\begin{aligned}\mathbb{F}^{(i,j)} |\psi_1\rangle \otimes \cdots \otimes |\psi_i\rangle \otimes \cdots \otimes |\psi_j\rangle \otimes \cdots \otimes |\psi_n\rangle \\ = |\psi_1\rangle \otimes \cdots \otimes |\psi_j\rangle \otimes \cdots \otimes |\psi_i\rangle \otimes \cdots \otimes |\psi_n\rangle \,,\end{aligned}$$

where $i, j \in \{1, 2, \ldots, n\}$. For $i = j$ we define $\mathbb{F}^{(i,i)} = \mathbb{1}$. Since $\left(\mathbb{F}^{(i,j)}\right)^2 = \mathbb{1}$, the eigenvalues of $\mathbb{F}^{(i,j)}$ are $+1$ and -1. A vector $|\psi_+\rangle$ which belongs to the eigenspace of $+1$ for all $\mathbb{F}^{(i,j)}$ describes a state which is invariant under interchange of subsystems, i.e. a bosonic state. Similarly, the intersection of all eigenspaces of -1 for the $\mathbb{F}^{(i,j)}$ with $i \neq j$ contains the fermionic states.[10] With this, we state the claim as

10 The intersections of all eigenspaces to eigenvalue $+1$ or to -1 of the flip operators are called the bosonic or fermionic »sectors«, respectively.

Lemma 3.10:
The output states ρ_{out} of symmetric covariant 1-to-n cloners for continuous-variable states lie in the bosonic sector, i.e. the output states have expectation value $+1$ with every flip operator, if and only if the cloner is described by a bosonic state ρ_T in (3.18). In particular,

$$\operatorname{tr}\big[\rho_{\text{out}}\,\mathbb{F}^{(i,j)}\big] = \operatorname{tr}\big[\rho_T\,\mathbb{F}^{(i,j)}\big] \text{ for } i,j \in \{1,2,\ldots,n\}\,.$$

Proof: To simplify notation, we understand $\rho \equiv \rho_{\text{out}}$ as the output state of a 1-to-n cloner described by a state ρ_T. Since we only consider deterministic cloners, the output states ρ are normalized anyway, $\operatorname{tr}[\rho] = 1$, and the proof can be restricted to flip operators $\mathbb{F}^{(i,j)}$ with $i \neq j$. To shorten expressions, we drop the phase space arguments of modes which are not considered and indicate the remaining modes by upper indices, e.g. for a characteristic function $\chi(\xi)$:

$$\chi^{(i,j)}(\xi,\eta) = \chi(\underbrace{0,\ldots,0,\xi}_{i},\underbrace{0,\ldots,0,\eta}_{j-i},0,\ldots,0)\,.$$

The same convention is used for other functions as well as Weyl operators and in a similar way for a single mode.

We start by discussing properties of $\mathbb{F} = \mathbb{F}^{(1,2)}$ for two modes and generalize later. In order to transport the action of $\mathbb{F}$ to phase space, note that

$$\mathbb{F}\,\mathrm{W}(\xi,\eta) = \mathrm{W}(\eta,\xi)\,\mathbb{F}\,. \tag{3.36}$$

We introduce the parity operator $\mathbb{P}^{(j)}$, which acts on the field operators of mode j by $\mathbb{P}^{(j)}\,R_k\,\mathbb{P}^{(j)} = -R_k$ for $k = 2j-1$ and $k = 2j$ in standard ordering of $\vec{R}$. On Weyl operators, $\mathbb{P}^{(j)}$ induces a change of sign for the respective argument,

$$\mathbb{P}^{(2)}\;\mathrm{W}(\xi,\eta) = \mathrm{W}(\xi,-\eta)\,\mathbb{P}^{(2)}.$$

Under a symplectic transformation S which maps two modes to symmetric and antisymmetric combinations according to

$$S\colon (\xi,\eta) \mapsto \left(\tfrac{\xi+\eta}{\sqrt{2}},\tfrac{\xi-\eta}{\sqrt{2}}\right),$$

$U_S^*\,\mathbb{F}\,U_S$ acts as $\mathbb{1}^{(1)} \otimes \mathbb{P}^{(2)}$:

$$\begin{aligned} U_S^*\,\mathbb{F}\,\mathrm{W}(\xi,\eta)\,U_S &= U_S^*\,\mathrm{W}(\eta,\xi)\,\mathbb{F}\,U_S \\ &= U_S^*\,\mathbb{F}\,U_S\,\mathrm{W}\big(\tfrac{\xi+\eta}{\sqrt{2}},\tfrac{\xi-\eta}{\sqrt{2}}\big) = \mathrm{W}\big(\tfrac{\eta+\xi}{\sqrt{2}},\tfrac{\eta-\xi}{\sqrt{2}}\big)\,U_S^*\,\mathbb{F}\,U_S\,. \end{aligned}$$

Hence the expectation value of $\mathbb{F}^{(i,j)}$ can be written as an expectation value of $\mathbb{1}^{(i)} \otimes \mathbb{P}^{(j)}$,

$$\operatorname{tr}\big[\rho\,\mathbb{F}^{(i,j)}\big] = \operatorname{tr}\big[\rho'\,\mathbb{1}^{(i)} \otimes \mathbb{P}^{(j)}\big],\ \text{where } \rho' = U_{S^{(i,j)}}^*\,\rho\,U_{S^{(i,j)}} \tag{3.37}$$

and $S^{(i,j)}$ acts on modes i and j.

Recall that by (2.15) the expectation value of $\mathbb{P}$ in ρ is obtained from the Wigner function, which in turn by (2.14) is a classical Fourier transform of χ_ρ:

$$\begin{aligned}\operatorname{tr}[\rho\,\mathbb{P}] &= \pi^f\,\mathcal{W}_\rho(0)\,,\\ \mathcal{W}_\rho(\xi) &= (2\pi)^{-2f}\int \mathrm{d}\eta\;\mathrm{e}^{\mathrm{i}\xi^{\mathrm{T}}\cdot\sigma\cdot\eta}\,\chi_\rho(\eta)\,.\end{aligned}$$

Hence

$$\begin{aligned}\operatorname{tr}\big[\rho'\,\mathbb{1}^{(i)}\otimes\mathbb{P}^{(j)}\big] &= (2\pi)^{-2f}\int \mathrm{d}\eta\;\chi^{(i,j)}_{\rho'}(0,\eta)\\ &= (2\pi)^{-2f}\int \mathrm{d}\eta\;\chi^{(i,j)}_{\rho}\big(\eta/\sqrt{2},-\eta/\sqrt{2}\big)\,,\end{aligned} \tag{3.38}$$

where

$$\chi^{(i,j)}_{\rho'}(0,\eta)=\operatorname{tr}\big[\rho'\;\mathrm{W}^{(i,j)}(0,\eta)\big]=\operatorname{tr}\Big[\rho\;\mathrm{W}^{(i,j)}\big(\tfrac{\eta+\xi}{\sqrt{2}},\tfrac{\eta-\xi}{\sqrt{2}}\big)\Big]=\chi^{(i,j)}_{\rho}\big(\tfrac{\eta+\xi}{\sqrt{2}},\tfrac{\eta-\xi}{\sqrt{2}}\big)\,.$$

Since ρ is the output state of a cloner determined by a state ρ_T, its characteristic function can be decomposed into $\chi_\rho(\xi)=t(\xi)\,\chi_{\mathrm{in}}(\sum_i\xi_i)=\chi_T(\Omega\,\xi)\,\chi_{\mathrm{in}}(\sum_i\xi_i)$ according to (3.16) and (3.17). Continuing (3.38), this yields

$$\begin{aligned}\operatorname{tr}\big[\rho'\,\mathbb{1}^{(i)}\otimes\mathbb{P}^{(j)}\big] &= (2\pi)^{-2f}\int \mathrm{d}\eta\;t^{(i,j)}\big(\eta/\sqrt{2},-\eta/\sqrt{2}\big)\,\chi_{\mathrm{in}}\big(\eta/\sqrt{2}-\eta/\sqrt{2}\big)\\ &= (2\pi)^{-2f}\int \mathrm{d}\eta\;\chi^{(i,j)}_{T}\big(\eta/\sqrt{2},-\eta/\sqrt{2}\big)\,.\end{aligned} \tag{3.39}$$

Note that $\chi_{\mathrm{in}}(0)=1$ and furthermore, Ω^{-1} from (3.22) has been applied to the argument of t together with a suitable substitution for η. Traveling back along the lines of (3.39), (3.38) and (3.37) for ρ and ρ_T, we get

$$\operatorname{tr}\big[\rho\,\mathbb{F}^{(i,j)}\big]=\operatorname{tr}\big[\rho'\,\mathbb{1}^{(i)}\otimes\mathbb{P}^{(j)}\big]=\operatorname{tr}\big[\rho'_T\,\mathbb{1}^{(i)}\otimes\mathbb{P}^{(j)}\big]=\operatorname{tr}\big[\rho_T\,\mathbb{F}^{(i,j)}\big]\,. \qquad \square$$

We now prove that all optimized symmetric cloners which were discussed in this chapter are described by a bosonic state ρ_T. Hence their output states are bosonic, too. Starting with the optimal joint fidelity cloner from Section 3.4.1, note that the fidelity operator F_{joint} commutes with all flip operators $\mathbb{F}^{(i,j)}$: The flip acts by interchanging the phase space arguments of modes i and j, see (3.36), and the Gaussian characteristic function $\exp(-\xi^{\mathrm{T}}\cdot\Gamma\cdot\xi/4)$ describing F_{joint} is invariant with respect to interchange of modes since its covariance matrix Γ from (3.26) is invariant. Hence the eigenvectors of F_{joint} are eigenvectors to all flip operators $\mathbb{F}^{(i,j)}$. But since the eigenstate to the maximal eigenvalue is pure and unique (cf. Section 3.4.1), it must be an eigenvector with eigenvalue $+1$ for all flips and thus lies in the bosonic sector.

The weighted, symmetric single-copy fidelity is represented by an operator $F = \sum_i F_i$, where $F_i = \exp(-P_i^2/2 - \sum_{i\neq j} Q_j^2/2)$ from (3.28). This operator is invariant under permutations of the modes and thus commutes with all flip operators $\mathbb{F}^{(i,j)}$. Just as for the joint fidelity, its eigenvectors are eigenvectors to the flip operators. For the optimal symmetric 1-to-2 cloner, the eigenvector to the maximal eigenvalue is unique by the arguments given in Section 3.4.2 (see discussion of the numerical optimization). Hence it is an eigenvector with eigenvalue $+1$ for all flip operators and thus bosonic.

Symmetric Gaussian 1-to-n cloners are described by a state ρ_T with characteristic function $\chi_T(\Omega\,\xi) = \exp\bigl(-\xi^{\mathrm{T}} \cdot (a\,\mathbb{1}_n \otimes \mathbb{1}_2 + b\,\mathbb{E}_n \otimes \mathbb{1}_2) \cdot \xi/4\bigr)$ by (3.31). Applying the transformation Ω^{-1} from (3.22) to the covariance matrix shows that the state commutes with all permutations of modes. By the above arguments, ρ_T as well as the output of the cloner is thus bosonic for all a and b. In particular, this is true for the best symmetric Gaussian 1-to-n cloner with $a = 1$, $b = (n-1-a)/n$ (cf. Section 3.4.2) and the best classical cloner with $a = 1$, $b = 1$ (cf. Section 3.4.3). These results are summarized in

Proposition 3.11:
The optimal joint fidelity cloner, the optimal 1-to-2 cloner, the best symmetric Gaussian 1-to-n cloners and the best classical cloners are described by a bosonic state ρ_T in (3.18) and thus yield bosonic output states by Lemma 3.10.

3.5 Optical implementation

An implementation of the optimal 1-to-2 cloners for single-copy and joint fidelity was briefly described by Cerf and Navez in [a]. A more detailed discussion is provided in e.g. [47, 48]. For reference and completeness, we sketch their ideas in this section. Note that optical implementations of the best symmetric Gaussian cloners have been described in [49] as well as in [50], where also the best asymmetric Gaussian 1-to-2 cloner is discussed.

The implementation is based on an optical parametric amplifier (OPA). In the setup depicted in Fig. 3.3 (taken from [a], see also [47]), it effectively acts as a linear amplifier [52] of intensity gain 2 for the signal in a_{in}, mixing in one part of the state ψ as the idler in b_1. This results in a signal output described by the annihilation operator $a'_{\mathrm{in}} = \sqrt{2}\,a_{\mathrm{in}} + b_1^*$ (not indicated in the picture). The idler output, given by $b'_1 = \sqrt{2}\,b_1 + a_{\mathrm{in}}^*$, is discarded. The signal is then mixed with the other part of ψ in b_2 at the beam splitter BS. Its output constitutes the two clones in modes a_1 and a_2. The state ψ characterizes the cloner and is equivalent to ρ_T in Eq. (3.17) and (3.23).

In the simplest setting, ψ is the vacuum state. This corresponds to the best symmetric Gaussian cloner [49, 50]. For the general case, the input–output relations of the system yield as annihilation operators for the output modes

$$a_1 = a_{\mathrm{in}} + (b_1^* + b_2)/\sqrt{2}\,,$$
$$a_2 = a_{\mathrm{in}} + (b_1^* - b_2)/\sqrt{2}\,.$$

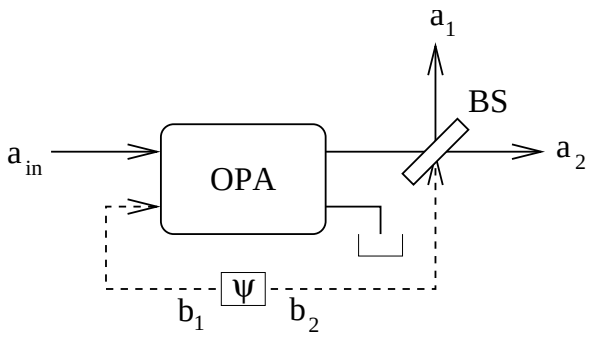


Figure 3.3:
Optical scheme of a displacement-covariant cloner. The input mode a_{in} is injected on the signal mode of an optical parametric amplifier (OPA) of gain 2, the idler mode being denoted as b_1. After amplification, the signal mode is divided at a balanced beam splitter (BS), resulting in two clones in modes a_1 and a_2. The second input mode of the beam splitter is noted b_2. If both b_1 and b_2 are initially in the vacuum state, the corresponding cloner is the Gaussian cloner of [53,54,55]. In contrast, if we inject a specific two-mode state $|\psi\rangle$ into b_1 and b_2, we can generate the whole set of displacement-covariant cloners, in particular the non-Gaussian optimal one. Picture and caption are taken from [a].

If the input state is the vacuum state $|0\rangle\langle 0|$, the single-copy fidelities are the expectation values of the operators

$$F_1 = \mathrm{e}^{-(Q_1+Q_2)^2/4-(P_1-P_2)^2/4}\,,$$
$$F_2 = \mathrm{e}^{-(Q_1-Q_2)^2/4-(P_1-P_2)^2/4}$$

in the state $|\psi\rangle\langle\psi|$. These operators differ from those in Eq. (3.29a) only by the symplectic transformation which describes the action of a beam splitter, i.e. by the mapping $a_1 \mapsto (a_1 + a_2)/\sqrt{2}$ and $a_2 \mapsto (a_1 - a_2)/\sqrt{2}$, resulting in

$$Q_1 \mapsto (Q_1 + Q_2)/\sqrt{2}\,, \qquad P_1 \mapsto (P_1 - P_2)/\sqrt{2}\,,$$
$$Q_2 \mapsto (Q_1 - Q_2)/\sqrt{2}\,, \qquad P_2 \mapsto (P_1 + P_2)/\sqrt{2}\,.$$

Cerf and Navez [a] argue that it is not necessary to implement the exact state $\rho_T = |\psi\rangle\langle\psi|$ to get substantial improvements over the fidelities of a Gaussian cloner. Already an approximation of the optimal state by a linear combination of a small number of few-photon states yields fidelities which clearly exceed the Gaussian limit. For example, the exact state for the symmetric cloner,

$$|\psi\rangle = \sum_{n=0}^{\infty} c_n\, |2n\rangle|2n\rangle\,, \tag{3.40}$$

can be truncated at $n = 2$ with $f_1 = f_2 \approx 0.6801$ compared to $f_1 = f_2 = \frac{2}{3}$ for the best Gaussian cloner, which is obtained for $n = 0$.

While this scheme is conceptually clear, it relies on a nonlinear interaction in the OPA, which poses difficulties in the experimental realization. Recently, Leuchs et al. [56] have proposed a scheme to realize the best symmetric Gaussian cloner based on linear quantum optical elements alone, namely beam splitters and homodyne detection. Their experiment implementing this scheme for 1-to-2 cloning was reported to yield estimated fidelities of 0.643 ± 0.01 and 0.652 ± 0.01 for the two clones. An implementation of the optimal cloner has not yet been reported in the literature.

3.6 Teleportation criteria

The limits on cloning of coherent states constitute at the same time criteria which allow to ascertain the successful conduction of a continuous-variable teleportation experiment. In quantum information theory, teleportation is the task of transmitting an arbitrary, unknown quantum state by sending only classical information [57, 58, 59]. This is not possible without the help of entangled states shared between sender and receiver which provide sufficiently strong correlations. The process consists of three steps, cf. Fig. 3.4: The sender, conventionally named Alice, performs a measurement on the input system ρ_{in} and her part of the shared entangled resource ω. She communicates the (classical) outcome c to the receiver, called Bob. Depending on this result, he applies a suitable unitary transformation on his part of the entangled state and ideally gets back the original input state in ρ_{out}. Note that the measurement »destroys« the quantum information in the input state, i.e. the state of the joint system on Alice's side after the measurement does not convey any information about the input state anymore. For continuous-variable systems, a common protocol [59, 60] uses a two-mode squeezed state as the entanglement resource. It consists of measuring two commuting quadrature components of the joint system at Alice's side and applying the outcome as a phase space displacement on Bob's system.

The fidelity of the output with respect to the original input state is determined by the »quality« of the entanglement, i.e. its amount quantified by a suitable entanglement measure.[11] In the finite-dimensional case, perfect teleportation is in principle possible with maximally entangled states as a resource. For continuous-variable systems, the output only approximately resembles the input state, because a maximally entangled state does not exist in this case.[12] If entanglement were not required, the classical information could be stored and used to replicate the input state, i.e. clone it. Reversing this argument shows that if the fidelity of the output state is higher than the limit of classical cloning in Eq. (3.34), the process must indeed have used entanglement. This turns the classical cloning limit into a success criterion for

11 The relevant entanglement measure is the entanglement of formation; see [62] for the relation between fidelity and entanglement in continuous-variable teleportation.

12 Such states could be abstractly realized as infinitely entangled states [44]. However, these are not normal states, i.e. they cannot be described by a density matrix.

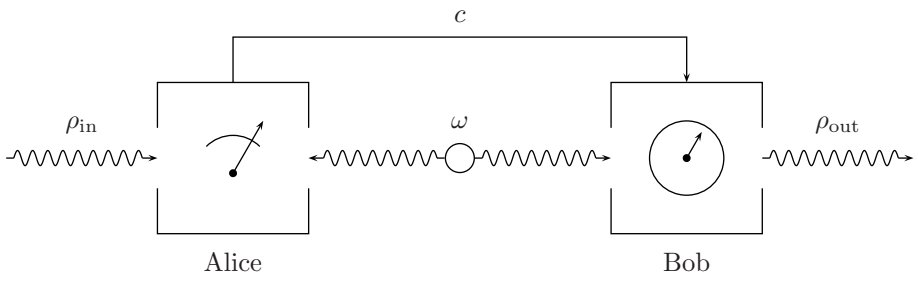


Figure 3.4:
Teleportation scheme: Alice and Bob share a bipartite entangled state ω. Alice performs a measurement on the input state ρ_{in} and her part of ω. She sends the classical outcome c to Bob, who adjusts his part of ω accordingly. This yields the output ρ_{out}.

continuous-variable teleportation. Until recently, the value of this bound was only assumed to be $\frac{1}{2}$ (though various papers provided ample evidence [60,63,64,65,66]). By the calculations in Section 3.4.3, published in [a], we could ascertain this value and thus prove the criterion. Moreover, since the derivation included procedures assisted by PPT-bound entanglement, we could even extend the criterion to this case:

Corollary 3.12:
A process that replicates a single input coherent state by measuring the input, forwarding classical information only and repreparing output states with a fidelity exceeding $\frac{1}{2}$ must have necessarily been assisted by non-PPT entanglement.

In [46] it has been proven in a more general context that the bound $f_{\text{classical}} \leq \frac{1}{2}$ is valid and tight for classical measure-and-prepare schemes where the fidelity is averaged over a flat distribution of input coherent states. For the standard teleportation protocol [59] involving only measurements of the quadrature components, i.e. the field operators Q_i and P_i, the findings of [60] imply that the maximum fidelity for teleportation of coherent states without supplemental entanglement is $\frac{1}{2}$. Our above result is more general as it does not make additional assumptions about the measure-and-prepare scheme and, moreover, distinguishes between PPT and non-PPT entanglement. Note, however, that teleportation of coherent states with the standard protocol can be described by a local-realistic model, cf. [60].

Another connection between cloning and teleportation concerns the distribution of quantum information. It is not necessarily clear that the output state of the teleportation process is the best remaining approximation to the input state. In fact, if the fidelity of the teleportation output is low, the input state might have not been used efficiently and still retain most of the information. However, if the fidelity of the output with respect to the original input state exceeds the single-copy fidelity of the optimal (non-Gaussian) 1-to-2 cloner, then the output system must

carry the best approximation to the input state since there can be no better clone in any other subsystem. This constitutes the second type of success criterion for continuous-variable teleportation:

Corollary 3.13:
If the fidelity of a teleported coherent state with respect to the original input state exceeds a value of $f \approx 0.6826$, the output system is the best remaining clone of the input state.

Of course, by Corollary 3.12, this teleportation process must have been assisted by non-PPT entanglement. A similar result has been obtained in [65]; while it is based on the same argument, it considers only the best Gaussian cloner with fidelity $\frac{2}{3}$.

Until recently, experimental teleportation of coherent states reached fidelities just below $\frac{2}{3}$, the fidelity of the best Gaussian 1-to-2 cloner. For example, the seminal experiment of Furusawa et al. [66] yielded fidelities of 0.58 ± 0.02. Later, Bowen et al. [67] reached fidelities of 0.64 ± 0.02 and Zhang et al. [68] reported fidelities of 0.61 ± 0.02. Only recently, Furusawa et al. [69] achieved a fidelity of 0.70 ± 0.02, surpassing both the Gaussian and the optimal limit.

Quantum Cellular Automata

4 Gaussian quantum cellular automata

This chapter presents an approach to characterize a quantum version of cellular automata which is based on continuous-variable systems and equipped with a quasi-free dynamics. For the general concept of quantum cellular automata we follow the lines of Schumacher and Werner [70].

A cellular automaton (CA) is a discrete, regular, dynamical system with synchronous, uniform time evolution generated by a local interaction. The dynamics acts on an infinite lattice, exhibits translational symmetry and has finite propagation speed. These characteristics render them a useful tool for the simulation of dynamical systems of regularly arranged, discrete, identical constituents. Within physics classical CAs have been employed to study problems in particular from statistical mechanics, e.g. Ising spin dynamics, point particle gases, percolation or annealing [71]. Other problems include the dynamics of bacteria colony growth, forest fires, sand piles or road traffic. Moreover, in classical information theory CAs are a model of universal computation, since a Turing machine can be simulated by a CA. And finally, CAs can provide diversion, e.g. in the form of John Conway's »Game of Life« [72]. Due to these applications the concept of a quantum cellular automaton (QCA), i.e. a quantum system with the above characteristics, seems to promise exciting possibilities. In fact, such a quantum extension of CAs has already been considered by R. Feynman in his paper on the power of quantum computation from 1982 [73]. Different notions of QCAs were studied in the literature and found to be capable of universal quantum computation [74, 75, 76, 77, 78]. And recently, Vollbrecht et al. [79, 80] have introduced a scheme for reversible, universal quantum computing in translationally invariant systems which proved to be a QCA.

While the development of a universal quantum computer is perhaps the most ambitious aim of quantum information science, it is at the same time possibly the most difficult undertaking (especially for interesting input problem size). However, specific computational tasks might be more easy to accomplish but nevertheless very useful from the point of view of general physics, e.g. the simulation of quantum systems. Since Hilbert space dimension grows exponentially with the number of constituents, classical computers face serious performance problems even for moderate system sizes. This obstacle could be overcome by quantum computers which convert the scaling into a feature. Even the simulation of quantum toy models with moderate system size could provide valuable insight into real-world systems. The inherent translational symmetry would make QCAs especially suited for the simulation of models in solid state physics.

In addition, the concept of a QCA might prove useful for the realization of quantum computing in optical lattices [81] and arrays of microtraps [82]. The experimental technology of these systems is quite highly developed and they are promising

candidates for the successful realization of a quantum computing device; in particular, they can be scaled to considerable systems sizes. However, most quantum computing concepts today require the individual addressing of specific constituents, e.g. qubits within the system, which is difficult in these approaches. It is much more feasible to change external parameters for the whole system, which is exactly a characteristic of a CA. As the essence of these arguments, we believe that quantum cellular automata are a promising concept which should not be neglected in the process of designing and developing systems capable of performing quantum computation.

We will in the following deal with Gaussian quantum cellular automata, i.e. a continuous-variable quantum system with the above characteristics of a CA. As a motivation to their study, consider the application of simulating a one-dimensional quantum random walk [83] on a QCA. In the most simple case of a random walk, a single »particle« or excitation moves from a starting cell to one of the neighboring sites. The direction of each step is determined randomly, e.g. by »flipping a coin« in the one-dimensional case. This dynamics is perfectly suited for implementation on a CA since the particle moves in steps within a finite neighborhood. From many repetitions of the walk with identical initial conditions, one obtains a distribution of final positions for the particle. In a quantum random walk, the states of the particle and the coin can be coherent superpositions. A unitary evolution maps the state of the coin onto the direction of the particle and moves it to the neighboring cell on the left or right accordingly. The outcome of a single run over several steps is a distribution of final positions of the particle in dependence of the initial conditions and the number of steps. In a realization on a QCA, each cell could correspond to the combination of a »slot« to host the particle and a »coin« to flip for the direction of the next step. If a particle is present in the respective cell, the dynamics of the QCA unitarily maps the state of the coin onto the direction of the particle and moves it to the neighboring cell on the left or right accordingly. Running the QCA from an initial state with one particle and the coins on every site in a coherent superposition of »left« and »right« then results in a quantum random walk on the line.

An obvious extension of this model to *quantum diffusion* is to populate the lattice with additional particles. However, in this case it is necessary to specify the treatment of collisions between particles. One possible solution limits the number of particles per site to a maximum of one particle moving left and one moving right. This corresponds to a »hard core interaction«, i.e. particles are not allowed to share sites but bounce off each other upon collision. Another solution allows for an arbitrary number of particles per site by second quantization of the random walk. This attaches to every cell a Fock space equipped with an occupation number state basis. Equivalently, every cell can be described as a quantum harmonic oscillator in an excited state according to the number of particles occupying the cell. The movement of particles over the lattice corresponds to the exchange of excitations between the oscillators. Together with a dynamics which can be implemented or approximated by a quadratic Hamiltonian, this bosonic system naturally gives rise to Gaussian QCAs, i.e. continuous-variable QCAs which map Gaussian states onto Gaussian states in the Schrödinger picture and which start from a Gaussian initial state. Examples of Gaussian QCAs include the free evolution, the »left-« and »right-shifter«, a contin-

ued squeezing (see below) and symplectic rotations. An experimental realization of a Gaussian QCA might use the vibrational degrees of freedom of atoms in an optical lattice.

Our principle aim in this chapter is to discover and access irreversibility in QCAs for the case of Gaussian systems. We prove that conceptually simple *reversible* Gaussian QCAs exhibit signs of irreversibility. Moreover, we examine the conceptual problems in the definition of irreversible QCAs, which become especially clear in the Gaussian case. In the long run, such QCAs could be employed to simulate ground states of other systems; by tuning global parameters of their dynamics, they could robustly drive a range of initial states into a limit state corresponding to a different Hamiltonian. We set out with a brief discussion of the definition and properties of a quantum analog of (deterministic) CAs along the lines of [70], including the problem of quantizing them in the first place. The remaining part of this chapter is devoted to Gaussian quantum cellular automata and the special instance of a one-dimensional chain of harmonic oscillators complete with Gaussian dynamics and Gaussian initial states. We present methods to deal with an infinite number of modes and investigate this system by decomposition into plane-wave modes. As a result, we show that the system exhibits properties typically related to irreversibility: Although the system evolves from a pure, uncorrelated state under a reversible dynamics, the correlation function describing the state converges. Moreover, this implies convergence in trace norm of the density operators describing the state for finite regions of the lattice. The reflection symmetric limit states are thermal equilibrium states determined by the correlation function of a pure state and a modewise temperature parameter. The last section examines the conceptual problems in the definition of irreversible QCAs, even in the Gaussian case. In particular, we present different concepts of localization and their impact on the definition of QCAs.

The contents of this chapter have in part been published in [b].

4.1 Quantum cellular automata

This section introduces the concept of QCAs formally and briefly presents some general results. In both we closely follow Schumacher and Werner [70].

Repeating the above characterization, a cellular automaton (CA) is a discrete, regular system with uniform dynamics arising from a local interaction. Abstractly, it is realized as an infinite lattice of identical, finite systems, where each cell is coupled to the sites in its neighborhood by a uniform dynamics called *local transition rule*. The neighboring cells are determined from a uniform, finite *neighborhood scheme* relative to any cell. While this scheme can be arbitrarily complex, it is mostly defined in the usual sense as the nearest or next-nearest neighbors of a cell. The time evolution of the whole system, the *global rule*, is discrete and synchronous. These properties imply a finite propagation speed. While a QCA is essentially a CA where the cells are (identical) quantum systems, there are some points to clarify.

Since our notion of a quantum cellular automaton is based on an infinite lattice, any attempt to define a QCA has to deal with the infinite number of quantum systems at the lattice sites. As discussed in [70], several previous definitions found in the literature suffer from conceptual shortcomings which prevent a successful application to infinite lattice systems. In particular, the notion of localization as implemented by states on the infinite lattice is problematic. For example, the basic operation of applying the same unitary transformation to each cell separately would require the multiplication of an infinite number of phase factors, which does not allow for a well-defined unitary operator describing the global state change.

In order to circumvent these problems, we work in the Heisenberg picture and define the dynamics of observables. This approach was motivated by methods used in statistical mechanics of quantum spin systems, where infinite arrays of simple quantum systems play a prominent role [70]. In contrast to a notion of localized states, localized observables are clearly defined: they require a measurement of a finite collection of cells only. If the lattice sites are labeled by s-tuples of integers, where s is the lattice dimension, we denote by $\mathcal{A}_x$ the algebra of observables which are localized on the single lattice site $x \in \mathbb{Z}^s$. This algebra could be an algebra of $d \times d$ matrices for a spin system or a CCR algebra for a continuous-variable system. The set of all observables which are localized on a finite region $\Lambda \subset \mathbb{Z}^s$ of the lattice constitutes the algebra $\mathcal{A}(\Lambda) = \bigotimes_{x\in\Lambda} \mathcal{A}_x$ associated with this region. For two regions $\Lambda_1 \subset \Lambda_2$, we take $\mathcal{A}(\Lambda_1)$ as a subalgebra of $\mathcal{A}(\Lambda_2)$ by tensoring with unit operators as necessary, i.e. on $\Lambda_2 \setminus \Lambda_1$. This allows us to properly define the product of two operators $A_1 A_2$ from different local algebras $\mathcal{A}(\Lambda_1)$ and $\mathcal{A}(\Lambda_2)$, respectively, as the corresponding element from $\mathcal{A}(\Lambda_1 \cup \Lambda_2)$. Since this procedure does not affect the norm, all local algebras are normed and their completion is the quasi-local algebra [84], denoted by $\mathcal{A}(\mathbb{Z}^s)$.

This inclusion of algebras is especially instructive in connection with the neighborhood. If $\mathcal{N} \subset \mathbb{Z}^s$ is defined as the finite neighborhood of the cell $x = 0$, we can install it as the uniform neighborhood scheme and obtain the neighborhood of any cell x as the set $x + \mathcal{N} \equiv \{x + n \mid n \in \mathcal{N}\}$. Accordingly, the neighborhood of a finite region $\Lambda \subset \mathbb{Z}^s$ of the lattice is the set $\Lambda + \mathcal{N} \equiv \{x + n \mid x \in \Lambda, n \in \mathcal{N}\}$. The observables on any finite region Λ are contained in the algebra on the region enlarged by its neighborhood, $\mathcal{A}(\Lambda) \subset \mathcal{A}(\Lambda + \mathcal{N})$, if and only if $\Lambda \subset \Lambda + \mathcal{N}$. This is only true if the neighborhood scheme explicitly contains the origin. While this need not necessarily be the case, we can formally enlarge the neighborhood without actually considering the additional elements in the interaction. Hence we can always assume $0 \in \mathcal{N}$. By the same argument, we can w.o.l.g. assume the neighborhood $\mathcal{N}$ to be simply connected. Note that by the above definition the »pointwise difference« of two sets is in general not empty, e.g. $\mathcal{N} - \mathcal{N} = \{x - y \mid x, y \in \mathcal{N}\}$.

The dynamics of the system is implemented as linear transformations on the observable algebras. In particular, one time step in the global evolution of the QCA is a transformation T on the observable algebra $\mathcal{A}(\mathbb{Z}^s)$ of the infinite system. To describe a proper time evolution, T has to be completely positive. Since we only consider deterministic dynamics, it has also to be unital, $T(\mathbb{1}) = \mathbb{1}$, i.e. it has to be a quantum channel. In addition, uniformity of the whole system requires that T

is translationally invariant. It has thus to commute with all lattice translations τ_x, where $x \in \mathbb{Z}^s$ and τ_x is the isomorphism from $\mathcal{A}_y$ to $\mathcal{A}_{y+x}$. Hence we have to require that $T(\tau_x A) = \tau_x T(A)$. If T is to arise from a local interaction coupling a cell to its neighborhood, it has to obey a suitable locality condition: For any observable A localized on a finite region Λ, the observable $T(A)$ obtained after one time step has to be localized in $\Lambda + \mathcal{N}$:

$$T\big(\mathcal{A}(\Lambda)\big) \subset \mathcal{A}(\Lambda + \mathcal{N}). \tag{4.1}$$

While T implements the global rule, i.e. one time step of the whole system, the local rule as the time evolution of a single cell x is obtained as the restriction T_x of T to this cell. Due to the translational invariance, it suffices to consider the origin; hence given T, the local rule is determined as $T_0 \colon \mathcal{A}_0 \to \mathcal{A}(\mathcal{N})$. A QCA is called reversible if the global rule T has an inverse which also is a quantum channel. This is equivalent to T being an automorphism of the quasi-local algebra. The above considerations give rise to the following definition of a QCA:

Definition 4.1:
A (deterministic) *quantum cellular automaton* (QCA) on the lattice $\mathbb{Z}^s$ with finite neighborhood scheme $\mathcal{N} \subset \mathbb{Z}^s$, where $0 \in \mathcal{N}$, is a quantum channel $T \colon \mathcal{A}(\mathbb{Z}^s) \to \mathcal{A}(\mathbb{Z}^s)$ on the quasi-local algebra which is translationally invariant and satisfies the locality condition $T\big(\mathcal{A}(\Lambda)\big) \subset \mathcal{A}(\Lambda + \mathcal{N})$ for every finite region $\Lambda \subset \mathbb{Z}^s$. A QCA is called *reversible* if T is an automorphism of $\mathcal{A}(\mathbb{Z}^s)$. While T constitutes the *global rule*, the *local rule* is its restriction to a single cell, $T_0 \colon \mathcal{A}_0 \to \mathcal{A}(\mathcal{N})$.

This definition essentially complies with the respective definition from [70]. However, we do not restrict it to reversible QCAs. Moreover, a QCA can be proven to be reversible if T is only a homomorphism.[1] For an extended discussion, including QCAs on finite lattices, see [70]. The elements of this definition correspond to the characteristics of a CA given at the beginning of this section as follows:

- ▷ lattice of discrete cells: an infinite lattice labeled by $x \in \mathbb{Z}^s$ with local observable algebras $\mathcal{A}_x$
- ▷ discrete, synchronous global time evolution: a quantum channel $T \colon \mathcal{A}(\mathbb{Z}^s) \to \mathcal{A}(\mathbb{Z}^s)$ on the quasi-local algebra $\mathcal{A}(\mathbb{Z}^s)$
- ▷ uniformity: translational invariance of T
- ▷ locality and finite propagation speed: for every finite set $\Lambda \subset \mathbb{Z}^s$ and the algebra of observables $\mathcal{A}(\Lambda)$ localized on this region, $T\big(\mathcal{A}(\Lambda)\big) \subset \mathcal{A}(\Lambda + \mathcal{N})$ with the finite neighborhood scheme $\mathcal{N}$
- ▷ local transition rule: the restriction of T to a single site, $T_0 \colon \mathcal{A}_0 \to \mathcal{A}(\mathcal{N})$
- ▷ reversibility: T is an automorphism.

1 This is a corollary of the *structure theorem* for reversible QCAs [70], which states that the inverse in this case is again a QCA.

While in this way the local rule can be directly inferred from the global rule, the definition of a particular QCA is not constructive. One would possibly rather start with a prescribed neighborhood scheme together with a local interaction and obtain a global rule to match. We join the authors of [70] on that a satisfactory theory of QCAs should connect the global transition rule T and the local rule such that either can be uniquely inferred from the other. They argue that the class of global rules should have an axiomatic specification, with locality and the existence of a finite neighborhood scheme as the most important aspect. In contrast, the local rule should be characterized constructively. This is easily possible for reversible QCAs. For later reference, we provide the relevant Lemma 2 from [70] and its proof:[2]

Lemma 4.2:
For a reversible QCA, global and local rule are equivalent, i.e.

(i) The global automorphism T is uniquely determined by the local transition rule T_0.

(ii) An automorphism $T_0\colon \mathcal{A}_0 \to \mathcal{A}(\mathcal{N})$ is the transition rule of a reversible QCA if and only if for all $x \in \mathbb{Z}^s$ such that $\mathcal{N} \cap (\mathcal{N}+x) \neq \emptyset$ the algebras $T_0(\mathcal{A}_0)$ and $\tau_x\big(T_0(\mathcal{A}_0)\big)$ commute elementwise.

Remark: Note that for all $x \in \mathbb{Z}^s$ not affected by (ii), i.e. those with $\mathcal{N}\cap(\mathcal{N}+x) = \emptyset$, the algebras $T_0(\mathcal{A}_0)$ and $\tau_x\big(T_0(\mathcal{A}_0)\big)$ commute anyway, because $T_0(\mathcal{A}_0) \subset \mathcal{A}(\mathcal{N})$.

Proof: By translational invariance of T it suffices to consider T_0, since $T_x\colon \mathcal{A}_x \to \mathcal{A}(x+\mathcal{N})$ is recovered as $T_x(A_x) = \tau_x\, T_0\, \tau_{-x}(A_x)$. Because T is an automorphism, it can be expressed in terms of T_x: any finite tensor product $\bigotimes_{x\in\Lambda} A_x$ of one-site operators A_x gives rise to

$$T\big(\textstyle\bigotimes_{x\in\Lambda} A_x\big) = T\big(\prod_{x\in\Lambda} A_x\big) = \displaystyle\prod_{x\in\Lambda} T_x(A_x). \tag{4.2}$$

For the first equality sign we have identified $\mathcal{A}_x$ with a subalgebra of $\mathcal{A}(\Lambda)$ by tensoring with unit operators (see above) and the second identity is due to T being an automorphism. Since the operators on the right hand side have overlapping localization regions $x+\mathcal{N}$, their product cannot be replaced by a tensor product. However, the argument of T is a product of commuting operators, hence is the right hand side. The commutativity condition of (ii) is thus necessary.

It is also sufficient because if the factors $T_x(A_x)$ commute, their product is unambiguously defined. Moreover, every local observable can be expressed as a linear combination of finite tensor products. Consequently, Eq. (4.2) defines an automorphism on the quasi-local algebra, proving (i). □

The commutation relation in (ii) above is in fact a key to the notion of a QCA from [70]. While it is automatically satisfied for reversible QCAs, it becomes an issue for the irreversible case (cf. Section 4.3). We therefor illustrate it in Fig. 4.1

2 The lemma is slightly restated to match the modified definition of a QCA.

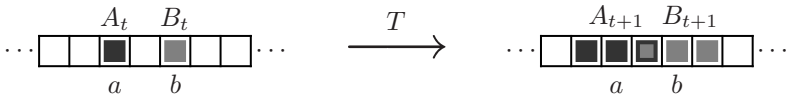


Figure 4.1:
One time step for a generic, one-dimensional nearest-neighbor QCA. Observables A_t and B_t are localized on different single sites, indicated by shaded cells. After one time step, implemented by applying the global rule T to the observables, their localization regions are enlarged by the neighborhood scheme $\mathcal{N} = \{-1, 0, 1\}$ and overlap.

for a generic QCA on a linear chain. For simplicity, we assume a nearest-neighbor interaction, i.e. the neighborhood scheme is $\mathcal{N} = \{-1, 0, 1\}$. At time t, consider two observables A_t and B_t which are localized on different, single sites a and b, respectively, two cells apart from each other. Then after one time step implemented by application of the global rule T the corresponding observables are A_{t+1} and B_{t+1}, which are localized on their original cell and its respective neighborhood, $a + \mathcal{N}$ and $b + \mathcal{N}$; hence their localization areas overlap at $a + 1 = b - 1$. The essence from the proof of Lemma 4.2 is the observation that the local rule T_0 determines the global rule if A_{t+1} and B_{t+1} commute on their overlap region, i.e. if in the example the restrictions $A_{t+1}\big|_{a+1}$ and $B_{t+1}\big|_{b-1}$ commute. This is necessarily true for reversible QCAs, but has to be imposed for the irreversible case.

As another important aspect of QCAs, it should be possible to concatenate two QCAs into a compound system, which again is a QCA. For reversible QCAs, this is assured as a consequence of the above lemma:

Corollary 4.3:
The concatenation of reversible QCAs is again a reversible QCA.

Proof: Consider two automorphisms $T_1, T_2 \colon \mathcal{A}(\mathbb{Z}^s) \to \mathcal{A}(\mathbb{Z}^s)$ which are global rules of reversible QCAs with isomorphic one-site algebras $\mathcal{A}_0$ and possibly different neighborhood schemes $\mathcal{N}_1$ and $\mathcal{N}_2$. The local rules are given by the restrictions $T_i\big|_0 \colon \mathcal{A}_0 \to \mathcal{A}(\mathcal{N}_i)$. A candidate for the local rule of the compound QCA is obtained as

$$T_0 \colon \mathcal{A}_0 \to \mathcal{A}(\mathcal{N}_1 + \mathcal{N}_2), \tag{4.3a}$$

$$T_0(A_0) = T_2\big(T_1\big|_0(A_0)\big) \tag{4.3b}$$

$$\begin{aligned} &= T_2\big(\textstyle\bigotimes_{y\in\mathcal{N}_1} B_y\big) = T_2\big(\prod_{y\in\mathcal{N}_1} B_y\big) \\ &= \textstyle\prod_{y\in\mathcal{N}_1} T_2\big|_y\big(B_y\big) \in \mathcal{A}(\mathcal{N}_1 + \mathcal{N}_2), \end{aligned} \tag{4.3c}$$

where we assumed that $T_1\big|_0(A_0) = \bigotimes_{y\in\mathcal{N}_1} B_y$ and used arguments from the proof of Lemma 4.2 for (4.3c). Since $T_1\big|_0$ and T_2 are automorphisms, T_0 is an automorphism

as well by (4.3b). In addition, T_0 inherits the necessary and sufficient commutation properties for application of Lemma 4.2 (ii) from $T_2\big|_0$. □

Again, this property becomes an issue for the concept of irreversible QCAs, see Section 4.3.

4.2 Reversible Gaussian QCA

A Gaussian quantum cellular automaton is a continuous-variable system which conforms to the Definition 4.1 of a QCA and evolves under a quasi-free dynamics, i.e. a dynamics that maps Gaussian states to Gaussian states in the Schrödinger picture. For the sake of clarity, we discuss our methods by means of a simple example system: an infinite one-dimensional chain of one-mode harmonic oscillators with nearest-neighbor coupling and translational invariance. The single-site algebras are thus isomorphic to the CCR algebra of one mode. Setting the lattice dimension $s = 1$, the quasi-local algebra becomes $\mathcal{A}(\mathbb{Z}^s) = \mathcal{A}(\mathbb{Z})$. While this restricts the generality of some of the results, the presented ideas are valid for arbitrary lattices with translational symmetry and a suitable elementary cell.[3] However, even for this restricted case there is an instance which exhibits the characteristics of irreversibility we are looking for (see Section 4.2.4).

4.2.1 Phase space and basics

While the rest of this thesis is concerned with Gaussian systems of finitely many modes, in this chapter the lattice structure requires a concept for infinitely many degrees of freedom. The phase space of such systems is an infinite-dimensional linear space of functions. Since we are interested in localized observables only and the CCR algebra is spanned by the Weyl operators, we can restrict ourselves to localized functions. Hence the phase space of the systems under consideration is the set $\Xi = \big\{\xi\colon \mathbb{Z} \to \mathbb{R}^2 \;\big|\; \xi_x \equiv \xi(x) = 0 \text{ almost everywhere}\big\}$, where $\mathbb{R}^2$ is the phase space of a single oscillator and the functions ξ vanish everywhere except for a finite number of sites. The global phase space »vectors« ξ relate every site x with a proper local phase space vector $\xi_x \in \mathbb{R}^2$ for a single mode. This generalizes the concept of a direct sum of one-site phase spaces to an infinite set of such systems. The symplectic form on this phase space is defined in terms of the symplectic form on the one-mode phase space, σ_s, as

$$\sigma(\xi, \eta) = \sum_{x \in \mathbb{Z}} \sigma_\mathrm{s}(\xi_x, \eta_x).$$

3 In [70], the authors argue that any QCA can be converted into a QCA with nearest-neighbor interaction at the expense of loosing full translational symmetry. We will not pursue this further, though.

4 To avoid too many indices, we write the arguments of Weyl operators in parentheses in this chapter, $\mathrm{W}(\xi) \equiv \mathrm{W}_\xi$.

Similarly, Weyl operators[4] $\mathrm{W}(\xi) \in \mathcal{A}(\mathbb{Z})$ on the whole system are defined as tensor products of single-site Weyl operators $w_x(\xi_x) \in \mathcal{A}_x$,

$$\mathrm{W}(\xi) = \bigotimes_{x\in\mathbb{Z}} w_x(\xi_x).$$

Both definitions are well-formed even on the infinite lattice, since the ξ_x are zero except for finitely many sites.

As we work in the Heisenberg picture, states are positive, normalized, linear functionals $\omega\colon \mathcal{A}(\mathbb{Z}) \to \mathbb{C}$ on the observable algebra, yielding a positive expectation value $\omega(A)$ for positive observables A. Alternatively, they can as usual be described by their characteristic function χ, the expectation value of all Weyl operators, $\chi(\xi) = \omega\big(\mathrm{W}(\xi)\big)$. For Gaussian states this is Gaussian and in strict analogy of Eq. (2.21)

$$\chi(\xi) = \exp\Big(-\tfrac{1}{4}\,\gamma(\xi,\xi) + \mathrm{i}\sum_{x\in\mathbb{Z}} \xi_x^{\mathrm{T}} \cdot d_x\Big).$$

Similar to the symplectic form, the covariances are contained in a bilinear correlation function $\gamma(\xi,\eta) = \sum_{x,z\in\mathbb{Z}} \xi_x^{\mathrm{T}} \cdot \gamma_{x,z} \cdot \eta_z$ defined as an effectively finite sum of terms involving (2×2 blocks of) covariance matrices for finitely many modes. The covariance matrix of a finite restriction of the chain is obtained as a block matrix of the respective $\gamma_{x,z}$. For example, the covariance matrix $\gamma|_{\{x,z\}}$ of two modes x and z is the 2×2 block matrix

$$\gamma|_{\{x,z\}} = \begin{pmatrix} \gamma_{x,x} & \gamma_{x,z} \\ \gamma_{z,x} & \gamma_{z,z} \end{pmatrix}.$$

For translationally invariant states, the displacement d_x has to be independent of the position in the chain, $d_x \equiv d$, and can be interpreted as a global »amplitude«. Likewise, the real 2×2 matrices $\gamma_{x,z}$ depend only on the distance between the two sites x and z, i.e. $\gamma_{x,z} = \gamma(x-z)$. Since the correlation function $\gamma(x)$ takes the role of the covariance matrix, it has to be symmetric, so we require $\gamma(-x) = \big(\gamma(x)\big)^{\mathrm{T}}$. A translationally invariant Gaussian state thus has a characteristic function of the form

$$\chi(\xi) = \exp\Big(-\tfrac{1}{4}\sum_{x,y\in\mathbb{Z}} \xi_x^{\mathrm{T}} \cdot \gamma(x-y) \cdot \xi_y + \mathrm{i}\sum_{x\in\mathbb{Z}} \xi_x^{\mathrm{T}} \cdot d\Big). \tag{4.4}$$

In order to describe an admissible Gaussian quantum state, the correlation function γ has to obey the state condition (2.22). The positivity condition $\gamma + \mathrm{i}\sigma \geq 0$ on matrices is in the present case replaced by the respective condition on bilinear functions, where complex-valued analogs to the phase space functions take the place of complex phase space vectors:

$$\gamma(\overline{\mu},\mu) + \mathrm{i}\sigma(\overline{\mu},\mu) \geq 0\,, \tag{4.5}$$

for all $\mu = \mu_{\mathrm{re}} + \mathrm{i}\mu_{\mathrm{im}}$ with $\mu_{\mathrm{re}}, \mu_{\mathrm{im}} \in \Xi$ and $\overline{\mu}$ as the complex conjugate. This condition stems from a direct generalization of the argument leading to (2.22). Writing

this out in components of μ and using the definitions of γ and σ above results in the detailed condition

$$\sum_{x,y\in\mathbb{Z}} \overline{\mu}_x^{\mathrm{T}} \cdot \big(\gamma(x-y) + \mathrm{i}\delta(x-y)\,\sigma_{\mathrm{s}}\big) \cdot \mu_y \geq 0 \tag{4.6}$$

for all μ as above. Here δ denotes the Kronecker delta with $\delta(x) = 1$ for $x = 0$ and $\delta(x) = 0$ otherwise.

4.2.2 Transition rule

To implement a Gaussian system, the global transition rule T has to be quasi-free, i.e. it has to map Gaussian states into Gaussian states in the Schrödinger picture. In the Heisenberg picture, this is accomplished by mapping the Weyl operators to Weyl operators subject to a symplectic transformation Γ:

$$T\big(\mathrm{W}(\xi)\big) = \mathrm{W}(\Gamma\,\xi). \tag{4.7}$$

Clearly, the so-defined T is a homomorphism, since

$$\begin{aligned} T\big(\mathrm{W}(\xi)\big)\,T\big(\mathrm{W}(\eta)\big) &= \mathrm{e}^{-\mathrm{i}\sigma(\Gamma\,\xi,\Gamma\,\eta)}\ \mathrm{W}(\Gamma\,\xi + \Gamma\,\eta) \\ &= \mathrm{e}^{-\mathrm{i}\sigma(\xi,\eta)}\ \mathrm{W}(\Gamma\,\xi + \Gamma\,\eta) = T\big(\mathrm{W}(\xi)\ \mathrm{W}(\eta)\big). \end{aligned}$$

It is also an automorphism, since as a symplectic transformation Γ is invertible. Hence together with a suitable locality condition T could indeed be the global rule of a Gaussian QCA. In fact, this is the only possible configuration: any transformation Γ resulting in a homomorphism would have to be linear in the arguments of the Weyl operators and fulfill $\sigma(\Gamma\,\xi, \Gamma\,\eta) = \sigma(\xi,\eta)$ for all ξ and η, which is exactly the definition of a symplectic transformation.

As with the generalization of matrices above, Γ acts on phase space functions by sitewise applying suitable real 2×2 matrices $\Gamma_{x,z}$,

$$(\Gamma\,\xi)_x = \sum_{z\in\mathbb{Z}} \Gamma_{x,z} \cdot \xi_z\,.$$

For T to be translationally invariant, i.e. invariant under lattice translations[5] τ_Δ, where $(\tau_\Delta\,\xi)_x = \xi_{x+\Delta}$ with $\Delta \in \mathbb{Z}$, the transformation Γ has to be invariant, too. It has thus to commute with τ_Δ for all $\xi \in \Xi$ and all $x, \Delta \in \mathbb{Z}$:

$$(\Gamma\,\tau_\Delta\,\xi)_x = (\tau_\Delta\,\Gamma\,\xi)_x \iff \Gamma_{x,z} = \Gamma_{x-z}\,.$$

We assume nearest-neighbor coupling for the example, which imposes $\Gamma_{x-z} = 0$ unless $|x-z| \leq 1$. Consequently, Γ is completely determined by three real-valued

5 We denote both the isomorphism of local algebras on different sites, $\tau_x\,\mathcal{A}_y = \mathcal{A}_{y+x}$, and the shifting of phase space functions, $(\tau_\Delta\,\xi)_x = \xi_{x+\Delta}$, by the same symbol τ. This is justified because both transformations represent the same change of origin of the lattice.

2×2 matrices $\Gamma_- \equiv \Gamma_{-1}$, $\Gamma_+ \equiv \Gamma_{+1}$ and Γ_0, acting on phase space functions as

$$(\Gamma\,\xi)_x = \sum_{z=-1}^{+1} \Gamma_z \cdot \xi_{x-z}\,. \tag{4.8}$$

Comparing this with a usual matrix, Γ might be depicted as an »infinite matrix« of the form

$$\Gamma = \begin{pmatrix} \ddots & & & & & & \\ 0 & \Gamma_+ & \Gamma_0 & \Gamma_- & 0 & & \\ & 0 & \Gamma_+ & \Gamma_0 & \Gamma_- & 0 & \\ & & 0 & \Gamma_+ & \Gamma_0 & \Gamma_- & 0 \\ & & & & & & \ddots \end{pmatrix}.$$

To express that Γ has to be symplectic, $\sigma(\Gamma\,\xi, \Gamma\,\eta) = \sigma(\xi,\eta)$, we make use of the symplectic transpose Γ^+ defined in Eq. (2.1) such that $\sigma(\Gamma\,\xi,\eta) = \sigma(\xi,\Gamma^+\eta)$ and $(\Gamma^+)_{x,z} = (\Gamma_{z,x})^+ = -\sigma_{\mathrm{s}} \cdot (\Gamma_{z,x})^{\mathrm{T}} \cdot \sigma_{\mathrm{s}}$. A transformation Γ is symplectic if and only if

$$\Gamma^+\Gamma = \mathbb{1}\,. \tag{4.9}$$

Writing this in components of Γ yields the compound condition

$$\delta(u)\,\mathbb{1} = \sum_{x\in\mathcal{N}} \Gamma_x^+ \cdot \Gamma_{u+x} \quad \text{for all } u \in \mathbb{Z}\,. \tag{4.10}$$

For a nearest-neighbor interaction this results in

$$\delta(u)\,\mathbb{1} = \sum_{x=-1}^{+1} \Gamma_x^+ \cdot \Gamma_{u+x} = \Gamma_-^+ \cdot \Gamma_{u-1} + \Gamma_0^+ \cdot \Gamma_u + \Gamma_+^+ \cdot \Gamma_{u+1} \quad \text{for all } u \in \mathbb{Z}$$

and in detail imposes the conditions

$$u = 0 \;:\quad \Gamma_-^+ \cdot \Gamma_- + \Gamma_0^+ \cdot \Gamma_0 + \Gamma_+^+ \cdot \Gamma_+ = \mathbb{1}\,, \tag{4.11a}$$

$$u = +1\text{:}\qquad \Gamma_-^+ \cdot \Gamma_0 + \Gamma_0^+ \cdot \Gamma_+ = 0\,, \tag{4.11b}$$

$$u = -1\text{:}\qquad \Gamma_0^+ \cdot \Gamma_- + \Gamma_+^+ \cdot \Gamma_0 = 0\,, \tag{4.11c}$$

$$u = +2\text{:}\qquad \Gamma_-^+ \cdot \Gamma_+ = 0\,, \tag{4.11d}$$

$$u = -2\text{:}\qquad \Gamma_+^+ \cdot \Gamma_- = 0\,. \tag{4.11e}$$

(The conditions for $|u| \geq 1$ correspond exactly to the requirement that observables which overlap on $3 - |u|$ cells have to commute, as can be seen from the discussion of (4.38) in Section 4.3.) Note that all these conditions are manifestly invariant under common symplectic transformations, i.e. the choice of a symplectic basis: subjecting two matrices A and B to the same symplectic transformation S in the above equations is equivalent to a similarity transformation with S, since

$$(S^{\mathrm{T}}A\,S)^+\,(S^{\mathrm{T}}BS) = -\sigma\,S^{\mathrm{T}}A^{\mathrm{T}}S\,\sigma\,S^{\mathrm{T}}BS = S^{-1}A^+BS\,.$$

In the case of one mode per site, the requirements of (4.11) simplify readily: The conditions for $u = \pm 2$, meaning $\sigma(\Gamma_- \xi, \Gamma_+ \eta) = \sigma(\Gamma_+ \xi, \Gamma_- \eta) = 0$ for all $\xi, \eta \in \mathbb{R}^2$, imply that Γ_- and Γ_+ project onto the same, one-dimensional subspace of $\mathbb{R}^2$. Hence both are multiples of a common matrix $\Gamma_\pm$ with rank one. For any real 2×2 matrix M we get $M^+ \cdot M = (\det M)\, \mathbb{1}$ and thus immediately have $\Gamma_-^+ \cdot \Gamma_- = \Gamma_+^+ \cdot \Gamma_+ = 0$ as well as $\Gamma_0^+ \cdot \Gamma_0 = \mathbb{1}$ from the condition for $u = 0$. But for one mode, this is equivalent to Γ_0 being a symplectic matrix. If we choose the one-dimensional subspace of Γ_- and Γ_+ as the direction of the position variable,[6] we get

$$\Gamma_+ = \Gamma_- = f\, \Gamma_\pm \quad \text{with} \quad \Gamma_\pm = \begin{pmatrix} (\Gamma_0)_{2,1} & (\Gamma_0)_{2,2} \\ 0 & 0 \end{pmatrix}, \tag{4.12}$$

where f is a common, arbitrary, real-valued coupling parameter and $(\Gamma_0)_{i,j}$ denotes the respective matrix entries of Γ_0. The shape of $\Gamma_\pm$ is a consequence of the conditions for $u = \pm 1$. We summarize these results in

Proposition 4.4:
The quasi-free quantum channel

$$T\big(\mathrm{W}(\xi)\big) = \mathrm{W}(\Gamma\, \xi),$$

where Γ is translationally invariant by (4.8) and symplectic by the conditions in (4.11), results in a reversible QCA on an infinite linear chain of harmonic oscillators with nearest-neighbor interaction. For the case of one mode per site, the on-site transformation Γ_0 is symplectic and determines the interaction $\Gamma_\pm$, except for the coupling constant f, according to (4.12).

Remark: The fact that in this case the coupling is identical in both directions implies that the »left-« and »right-shifter« mentioned as examples in the introduction cannot be realized with one mode per site. Instead, they require a spare »swap« system and an alternating partitioning scheme in order to avoid collision problems. For details, see [70].

Proof: These definitions result in a QCA in the sense of Definition 4.1. The local observable algebra $\mathcal{A}_x$ is spanned by the Weyl operators on single lattice sites, $w_x(\xi_x)$ with $\xi_x \in \mathbb{R}^2$. The global Weyl operators $\mathrm{W}(\xi)$ with $\xi \in \Xi$ span the quasi-local algebra $\mathcal{A}(\mathbb{Z})$. Since Γ is a symplectic transformation and translationally invariant, T as defined above is a translationally invariant automorphism of $\mathcal{A}(\mathbb{Z})$. The requirement of locality and finite propagation speed is met by the nearest-neighbor coupling inherent in Γ. The local rule is the restriction of T to the algebra of single-site observables. □

A single time step of the system is implemented by applying T to the observable in question. For Weyl operators, this is by the definition in (4.7) the same as applying

6 This choice can be interpreted either as a specification of the interaction $\Gamma_\pm$ or as a choice of the symplectic basis in the phase space $\mathbb{R}^2$ of a single site.

Γ to the phase space argument ξ. Further iteration of the dynamics for t time steps is equivalent to an overall transformation $\Gamma_{t+1} = \Gamma\,\Gamma_t$. Due to the translational invariance, this is a convolution-style operation,

$$(\Gamma_{t+1})_{x,z} = (\Gamma_{t+1})_{x-z} = \sum_{y=-1}^{+1} \Gamma_{(x-z)-y} \cdot (\Gamma_t)_y \,. \tag{4.13}$$

4.2.3 Fourier transform

Since the system obeys translational invariance, it can be diagonalized together with the momentum operator generating the translations. Hence we can simplify expressions like the iteration relation (4.13) by turning to the Fourier transform of the phase space, i.e. we decompose the phase space elements ξ into plane-wave modes as the eigenstates of the momentum operator and consider the resulting weight functions $\hat{\xi}$ with values $\hat{\xi}(k) \in \mathbb{R}^2$:

$$\xi_x = \frac{1}{2\pi} \int_{-\pi}^{\pi} \mathrm{d}k\; \hat{\xi}(k)\, \mathrm{e}^{+\mathrm{i}kx} \quad \text{and} \quad \hat{\xi}(k) = \sum_{x\in\mathbb{Z}} \xi_x\, \mathrm{e}^{-\mathrm{i}kx} \,. \tag{4.14}$$

Due to the discrete structure, k is unique only up to multiples of 2π, hence the Fourier transform is determined by $k \in [-\pi, \pi]$. All other translationally invariant quantities are treated similarly. This casts the iteration relation (4.13) into an ordinary multiplication of matrices,

$$\hat{\Gamma}_t(k) = \big(\hat{\Gamma}(k)\big)^t, \quad \text{where } \hat{\Gamma}(k) = \Gamma_0 + 2f\cos(k)\,\Gamma_\pm \tag{4.15}$$

is the Fourier transform of Γ_x according to (4.14).

The Fourier transform also simplifies the state condition (4.6) for γ. To properly define the transformed $\widehat{\gamma}(k)$, we restrict $\gamma(x)$ to be absolutely summable, i.e. $\sum_{x\in\mathbb{Z}} \|\gamma(x)\| < \infty$. This condition excludes problematic correlation functions, e.g. those with singular portions but retains the important cases of product and clustering initial states. From a mathematical point of view, it requires $\gamma(x)$ to decrease faster than $1/|x|$ and makes $\widehat{\gamma}(k)$ continuous. With this, the state condition (4.6) on the correlation function reads in terms of Fourier transforms

$$\frac{1}{2\pi} \int_{-\pi}^{\pi} \mathrm{d}k\; \overline{\widehat{\mu}^{\mathrm{T}}(k)} \cdot \big(\widehat{\gamma}(k) + \mathrm{i}\sigma_{\mathrm{s}}\big) \cdot \widehat{\mu}(k) \geq 0. \tag{4.16}$$

This is equivalent to the condition on 2×2 matrices that $\widehat{\gamma}(k) + \mathrm{i}\sigma_{\mathrm{s}} \geq 0$ for all $k \in [-\pi, \pi]$: if this condition holds for all k, then the l.h.s. of (4.16) is indeed positive semi-definite; if, however, $\widehat{\gamma}(k_0) + \mathrm{i}\sigma_{\mathrm{s}}$ is not positive semi-definite for some k_0, then the l.h.s. of (4.16) can be made negative by choosing an appropriate $\widehat{\mu}(k)$, e.g. the sharply peaked Fourier transform of a flat Gaussian which is centered around k_0 and has been restricted to finite support. Moreover, if $\widehat{\gamma}(k_0) + \mathrm{i}\sigma_{\mathrm{s}}$ is strictly positive for

some k_0, this property will be spread out by inverse Fourier transform to the whole of $\gamma(x)$. In this case, γ determines the characteristic function of a pure Gaussian state plus additional Gaussian noise and therefore corresponds to a mixed state. Conversely, $\widehat{\gamma}(k)$ describes a pure Gaussian state if $\big(\sigma_\mathrm{s}\,\widehat{\gamma}(k)\big)^2 = -\mathbb{1}$ (cf. Section 2.2). The state condition on the bilinear form γ over the infinite chain is thus transformed into a condition of the same form on finite matrices under Fourier transform. This is summarized in the following

Lemma 4.5:
A function γ which maps $x \in \mathbb{Z}$ to real 2×2 matrices, is absolutely summable, $\sum_{x\in\mathbb{Z}}\|\gamma\| < \infty$, and symmetric, $\gamma(-x) = \big(\gamma(x)\big)^\mathrm{T}$,

(i) defines a translationally invariant Gaussian state on the linear chain labeled by $\mathbb{Z}$ if and only if the Fourier transform $\widehat{\gamma}(k)$ fulfills $\widehat{\gamma}(k) + \mathrm{i}\sigma_\mathrm{s} \geq 0$ for all $k \in [-\pi, \pi]$ and

(ii) corresponds to a pure Gaussian state if and only if $\widehat{\gamma}(k) + \mathrm{i}\sigma_\mathrm{s}$ is not strictly positive for any $k \in [-\pi, \pi]$, i.e. if $\big(\sigma_\mathrm{s}\,\widehat{\gamma}(k)\big)^2 = -\mathbb{1}$.

During time evolution of the system, the correlation function γ changes according to the symplectic transformation Γ of the phase space argument in (4.7) as

$$\gamma_t(x) = \sum_{y,z\in\mathbb{Z}} \big(\Gamma_t(y)\big)^\mathrm{T} \cdot \gamma_0(x+y-z) \cdot \Gamma_t(z) \quad \text{or} \tag{4.17a}$$

$$\widehat{\gamma}_t(k) = \overline{\hat{\Gamma}_t^\mathrm{T}(k)} \cdot \widehat{\gamma}_0(k) \cdot \hat{\Gamma}_t(k), \tag{4.17b}$$

where γ_0 denotes the correlation function of the initial state.

4.2.4 Example system

To gain more specific results, we consider a more concrete instance of the above system: The initial state is a coherent product state described by the correlation function $\gamma_0(0) = \mathbb{1}$ and $\gamma_0(x) = 0$ otherwise, resulting in the Fourier transform $\widehat{\gamma}_0(k) = \mathbb{1}$. Clearly, γ conforms to the requirements of Lemma 4.5 and thus describes a translationally invariant, *pure* Gaussian state. For the on-site part Γ_0 of the dynamics, we choose a rotation, $\Gamma_0 = \left(\begin{smallmatrix}\cos\phi & -\sin\phi \\ \sin\phi & \cos\phi\end{smallmatrix}\right)$, where $-\pi \leq \phi \leq \pi$, which by (4.12) determines Γ up to the coupling parameter f. Repeating (4.15) and (4.12), the Fourier transform is

$$\hat{\Gamma}(k) = \Gamma_0 + 2f\cos(k)\,\Gamma_\pm \quad \text{with } \Gamma_\pm = \begin{pmatrix}(\Gamma_0)_{2,1} & (\Gamma_0)_{2,2} \\ 0 & 0\end{pmatrix}. \tag{4.18}$$

Since $\Gamma_\pm$ contains a row of Γ_0, the determinant is $\det\hat{\Gamma}(k) = \det\Gamma_0 = 1$. Hence $\hat{\Gamma}(k)$ induces a symplectic transformation on every single mode k. The value of the coupling parameter f determines whether the two eigenvalues of $\hat{\Gamma}(k)$ are real and

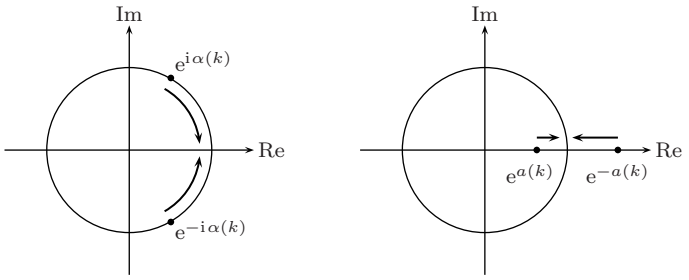


Figure 4.2:
Depicting the eigenvalues of $\hat{\Gamma}(k)$: for small coupling parameter $|f| < f_{\text{crit}}$ the two eigenvalues are complex phases and conjugated to each other (left figure); for large coupling $|f| > f_{\text{crit}}$, the eigenvalues are real and inverse to each other (right figure). All eigenvalues meet at a value of 1 for $f \to f_{\text{crit}}$.

inverse or complex and conjugate to each other.[7] To obtain a quantitative statement, we write the eigenvalues as $e^{\pm i\alpha(k)}$, where $\alpha(k)$ is either real- or purely imaginary-valued, and consider the trace as their sum:

$$\begin{aligned} \operatorname{tr}\hat{\Gamma}(k) = e^{i\alpha(k)} + e^{-i\alpha(k)} = 2\cos\alpha(k) = 2\cos\phi + 2f\cos(k)\sin\phi \\ \Rightarrow \alpha(k) = \arccos\bigl(\cos\phi + f\cos(k)\sin\phi\bigr). \end{aligned} \tag{4.19}$$

If $|\operatorname{tr}\hat{\Gamma}(k)| \leq 2$, then $\alpha(k)$ is real-valued, $|e^{\pm i\alpha(k)}| = 1$ and $\hat{\Gamma}(k)$ is a rotation on mode k. Otherwise, $\alpha(k)$ is purely imaginary-valued, the eigenvalues are real and $\hat{\Gamma}(k)$ corresponds to a squeezing. For $|\operatorname{tr}\hat{\Gamma}(k)| = 2$ the eigenvalues meet at a value of 1. The relevance of the eigenvalues lies in their direct consequence for the dynamics: if some $\hat{\Gamma}(k_0)$ had real eigenvalues larger than 1, the respective mode would be constantly squeezed, which would transform any input state over time into an »infinitely squeezed state« [44]. The limit state of such dynamics is highly singular; for example, the probability for any oscillator in the chain to be finitely excited is zero. The nonsqueezing regime with real eigenvalues for all $\hat{\Gamma}(k)$ is given by the inequality

$$\bigl|\cos\alpha(k)\bigr| = \bigl|\cos\phi + f\cos(k)\sin\phi\bigr| \leq 1\,,$$

which has to hold for all $k \in [-\pi, \pi]$. Except for cases where $\sin\phi = 0$ or $\cos(k) = 0$ and the above inequality is trivially true, the respective condition on f is

$$|f| \leq f_{\text{crit}} = \frac{1 - |\cos\phi|}{|\sin\phi|} \iff \begin{cases} |f| \leq \bigl|\tan(\phi/2)\bigr| \text{ for } |\phi| \leq \pi/2\,, \\ |f| \leq \bigl|\cot(\phi/2)\bigr| \text{ for } \pi/2 < |\phi| \leq \pi\,. \end{cases} \tag{4.20}$$

(Note that either none or both conditions hold, since $\bigl|\tan(\phi/2)\bigr| \leq \bigl|\cot(\phi/2)\bigr|$ for $|\phi| \leq \pi/2$ and vice versa.) In order to retain the possibility of finding (normal) limit

7 The general case of eigenvalues which are complex and *inverse* to each other is excluded since $\hat{\Gamma}(k)$ is real-valued. Hence the characteristic polynomial of $\hat{\Gamma}(k)$ has real coefficients and complex solutions are conjugated to each other.

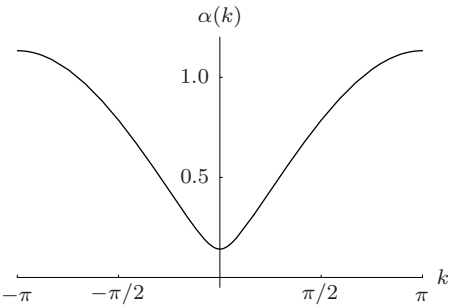


Figure 4.3:
Plot of $\alpha(k) = \arccos\bigl(\cos\phi + f\cos(k)\sin\phi\bigr)$ according to Eq. (4.19), for $f = 0.4$ and $\phi = \frac{\pi}{4}$.

states, we concentrate on the nondegenerate case of small couplings $|f| < \bigl|\tan(\phi/2)\bigr|$ or $|f| < \bigl|\cot(\phi/2)\bigr|$. The above relations between f and the eigenvalues are illustrated in Fig. 4.2; for a plot of the resulting $\alpha(k)$ see Fig. 4.3.

We will consider below the time evolution of the initial state, show that it converges and characterize the possible limit states. The following arguments make use of the projectors onto the eigenspaces of $\hat{\Gamma}$, which are provided by

Lemma 4.6:
If $\hat{\Gamma}(k)$ has nondegenerate, complex eigenvalues $\mathrm{e}^{\pm\mathrm{i}\alpha(k)}$ with $\alpha(k) \in (0,\pi)$, the (nonorthogonal) projectors P_k and $\overline{P_k}$ onto its eigenspaces in a decomposition

$$\hat{\Gamma}(k) = \mathrm{e}^{\mathrm{i}\alpha(k)}\, P_k + \mathrm{e}^{-\mathrm{i}\alpha(k)}\, \overline{P_k} \tag{4.21}$$

are given by

$$P_k = \tfrac{1}{2}\,\mathbb{1} + \tfrac{\mathrm{i}}{2}\,\bigl(\cos\alpha(k)\,\mathbb{1} - \hat{\Gamma}(k)\bigr)\,\bigl(\sin\alpha(k)\bigr)^{-1} \tag{4.22}$$

and $\overline{P_k}$ as the complex conjugate of P_k.

Proof: The operators P_k and $\overline{P_k} = \mathbb{1} - P_k$ are projectors onto the disjoint eigenspaces of $\hat{\Gamma}(k)$.[8] Since $P_k + \overline{P_k} = \mathbb{1}$, the real and imaginary parts of both projectors are connected via $\mathrm{Re}\,\overline{P_k} = \mathbb{1} - \mathrm{Re}\,P_k$ and $\mathrm{Im}\,\overline{P_k} = -\mathrm{Im}\,P_k$. Writing the above decomposition (4.21) in terms of $\mathrm{Re}\,P_k$ and $\mathrm{Im}\,P_k$ yields

$$\hat{\Gamma}(k) = \cos\alpha(k)\,\mathbb{1} - 2\sin\alpha(k)\;\mathrm{Im}\,P_k + \mathrm{i}\sin\alpha(k)\,(2\,\mathrm{Re}\,P_k - \mathbb{1}). \tag{4.23}$$

By (4.18), $\hat{\Gamma}(k)$ has to be real-valued. Hence the last term of (4.23) has to vanish and we immediately obtain $\mathrm{Re}\,P_k = \mathbb{1}/2$. Note that we excluded the degenerate

8 Proof of this statement: If ψ_- is the eigenvector of $\hat{\Gamma}(k)$ to eigenvalue $\mathrm{e}^{-\mathrm{i}\alpha(k)}$, then $\mathrm{e}^{-\mathrm{i}\alpha(k)}\,\psi_- = \hat{\Gamma}(k)\cdot\psi_- = \bigl(\mathrm{e}^{\mathrm{i}\alpha(k)}\,P_k + \mathrm{e}^{-\mathrm{i}\alpha(k)}\,(\mathbb{1} - P_k)\bigr)\cdot\psi_-$, which implies $P_k\cdot\psi_- = 0$ and $\overline{P_k}\cdot\psi_- = \psi_-$. Similarly, $P_k\cdot\psi_+ = \psi_+$ and $\overline{P_k}\cdot\psi_+ = 0$ for the eigenvector ψ_+ to eigenvalue $\mathrm{e}^{\mathrm{i}\alpha(k)}$. Since $\hat{\Gamma}(k)$ has determinant 1 and thus full rank, the eigenvectors are linearly independent and span the whole space $\mathbb{R}^2$. Hence $0 = P_k\cdot\overline{P_k} = P_k\cdot(\mathbb{1} - P_k) = P_k - P_k^2$ or $P_k^2 = P_k$, i.e. P_k is a projector. The same holds for $\overline{P_k}$.

case, which corresponds to $\sin\alpha(k) = 0$. The imaginary part is readily obtained from (4.23) as $\operatorname{Im} P_k = \big(\cos\alpha(k)\,\mathbb{1} - \Gamma(k)\big)/\big(2\sin\alpha(k)\big)$, which proves (4.22). For the remaining projector, we get $\operatorname{Re}\overline{P_k} = \operatorname{Re} P_k$ and $\operatorname{Im}\overline{P_k} = -\operatorname{Im} P_k$ from the beginning of the proof. Hence $\overline{P_k}$ is indeed the complex conjugate of P_k. □

Convergence

The decomposition (4.21) of $\hat\Gamma(k)$ is particularly useful for a compact description of the iterated transformation $\hat\Gamma_t(k)$. By (4.15),

$$\hat\Gamma_t(k) = \big(\hat\Gamma(k)\big)^t = \mathrm{e}^{\mathrm{i}t\alpha(k)}\,P_k + \mathrm{e}^{-\mathrm{i}t\alpha(k)}\,\overline{P_k}\,, \tag{4.24}$$

since as projectors on disjoint eigenspaces P_k and $\overline{P_k}$ obey $P_k^2 = P_k$, $\overline{P_k}^2 = \overline{P_k}$ and $P_k \cdot \overline{P_k} = 0$. With this relation, the time-dependent correlation function $\gamma_t(x)$ is obtained by inverse Fourier transform from (4.17) as

$$\begin{aligned}
\gamma_t(x) &= \frac{1}{2\pi}\int_{-\pi}^{\pi}\mathrm{d}k\;\mathrm{e}^{\mathrm{i}kx}\,\overline{\hat\Gamma_t^{\mathrm{T}}(k)}\cdot\widehat{\gamma}_0(k)\cdot\hat\Gamma_t(k)\\
&= \frac{1}{2\pi}\int_{-\pi}^{\pi}\mathrm{d}k\;\mathrm{e}^{\mathrm{i}kx}\left(\mathrm{e}^{2\mathrm{i}t\alpha(k)}\,P_k^{\mathrm{T}}\cdot\widehat{\gamma}_0(k)\cdot P_k + \mathrm{e}^{-2\mathrm{i}t\alpha(k)}\,\overline{P_k}^{\mathrm{T}}\cdot\widehat{\gamma}_0(k)\cdot\overline{P_k}\right)\\
&\quad + \frac{1}{2\pi}\int_{-\pi}^{\pi}\mathrm{d}k\;\mathrm{e}^{\mathrm{i}kx}\left(P_k^{\mathrm{T}}\cdot\widehat{\gamma}_0(k)\cdot\overline{P_k} + \overline{P_k}^{\mathrm{T}}\cdot\widehat{\gamma}_0(k)\cdot P_k\right).
\end{aligned} \tag{4.25}$$

In (4.25), the transformation is separated into a time-dependent, oscillating part in the first term and a stationary part in the second. In the limit of large time t, the rapidly oscillating term vanishes and the correlation function converges by an argument similar to the method of stationary phase: Starting from a product state (or any clustering state), $\widehat{\gamma}_0(k)$ is continuous; since we excluded the degenerate case, $\hat\Gamma(k)$, P_k and $\overline{P_k}$ are continuous, too, and the whole integrand is well-behaved. Note that $\alpha(k)$ is differentiable and has only finitely many extrema (cf. Fig. 4.3 and caption). The main contribution to the integral stems from intervals where $\alpha'(k) \approx 0$, i.e. from around the extrema of $\alpha(k)$ at k_n, ordered such that $k_n \le k_{n+1}$ for $n = 1, 2, \ldots N < \infty$. We explain the argument for the first term in the first integrand of (4.25). Splitting the integral at the extrema of $\alpha(k)$ at k_n and writing $\hat c(k) = P_k^{\mathrm{T}}\cdot\widehat{\gamma}_0(k)\cdot P_k$, we obtain:

$$\begin{aligned}
&\int_{-\pi}^{\pi}\mathrm{d}k\;\hat c(k)\exp\big(\mathrm{i}kx + 2\,\mathrm{i}t\alpha(k)\big) =\\
&\sum_{n=1}^{N}\underbrace{\int_{k_n-\epsilon}^{k_n+\epsilon}\mathrm{d}k\;\hat c(k)\exp\big(\mathrm{i}kx + 2\,\mathrm{i}t\alpha(k)\big)}_{\equiv A} + \sum_{n=1}^{N}\underbrace{\int_{k_n+\epsilon}^{k_{n+1}-\epsilon}\mathrm{d}k\;\hat c(k)\exp\big(\mathrm{i}kx + 2\,\mathrm{i}t\alpha(k)\big)}_{\equiv B} + R
\end{aligned}$$

where

$$R = \int_{-\pi}^{k_1-\epsilon} \mathrm{d}k\ \hat{c}(k) \exp\bigl(\mathrm{i}kx + 2\,\mathrm{i}t\alpha(k)\bigr) + \int_{k_N+\epsilon}^{\pi} \mathrm{d}k\ \hat{c}(k) \exp\bigl(\mathrm{i}kx + 2\,\mathrm{i}t\alpha(k)\bigr).$$

Integrals of type A cover intervals around the extrema of $\alpha(k)$, integrals B the intervals in between extrema. The other two integrals in R cover remainders at the ends of the whole integration interval $[-\pi, \pi]$; they are effectively of type B. If the derivative of $\alpha(k)$ is nonvanishing, $\alpha'(k) \neq 0$, we can substitute $u = 2\alpha(k)$ and $k = \alpha^{-1}(u)$ to obtain for integrals of type B:

$$\int_{k_n+\epsilon}^{k_{n+1}-\epsilon} \mathrm{d}k\ \hat{c}(k) \exp\bigl(\mathrm{i}kx + 2\,\mathrm{i}t\alpha(k)\bigr) = \bigl(2\alpha'(k)\bigr)^{-1} \int_{u_n}^{u'_n} \mathrm{d}u\ \hat{c}\bigl(\alpha^{-1}(u)\bigr) \exp\bigl(\mathrm{i}x\alpha^{-1}(u) + 2\,\mathrm{i}tu\bigr),$$

where $u_n = 2\alpha(k_n + \epsilon)$ and $u'_n = 2\alpha(k_{n+1} - \epsilon)$. Since this integrand is absolutely integrable, the Riemann-Lebesgue lemma [7, Ch. IX] assures that the integral vanishes for $t \to \infty$. For integrals A, this substitution is not possible since $\alpha'(k_n) = 0$. However, we can expand $\alpha(k)$ to second order around k_n, yielding

$$\int_{k_n-\epsilon}^{k_n+\epsilon} \mathrm{d}k\ \hat{c}(k) \exp\bigl(\mathrm{i}kx + 2\,\mathrm{i}t\alpha(k)\bigr) = \mathrm{e}^{2\mathrm{i}t\alpha(k_n)} \int_{k_n-\epsilon}^{k_n+\epsilon} \mathrm{d}k\ \hat{c}(k) \exp\bigl(\mathrm{i}kx + 2\,\mathrm{i}t(k-k_n)^2\alpha''(k_n)\bigr).$$

Again, the integral vanishes for $t \to \infty$. These arguments would be spoiled by any $\hat{\Gamma}(k_0)$ with real eigenvalues, which would turn the phase factor $\mathrm{e}^{2\mathrm{i}t\alpha(k)}$ into a real-valued exponential and thus result in continued squeezing of the respective mode. Hence we restrict the dynamics to small coupling parameter f.

While the correlation function $\gamma(x)$ converges, the amplitude part $\sum_{x\in\mathbb{Z}} \xi_x^{\mathrm{T}} \cdot d$ of a translationally invariant state in (4.4) does *not* unless $d = 0$: Under time evolution for t steps, the initial sum is mapped to

$$\begin{aligned}\sum_{x\in\mathbb{Z}} \xi_x \longmapsto \sum_{x\in\mathbb{Z}} (\Gamma_t\,\xi)_x &= \hat{\Gamma}_t(0) \cdot \hat{\xi}(0) \\ &= \bigl(\mathrm{e}^{\mathrm{i}t\alpha(0)}\,P_0 + \mathrm{e}^{-\mathrm{i}t\alpha(0)}\,\overline{P_0}\bigr) \cdot \hat{\xi}(0) = \bigl(\mathrm{Re}(\mathrm{e}^{\mathrm{i}t\alpha(0)}\,P_0)\bigr) \cdot \hat{\xi}(0).\end{aligned}$$

This expression clearly depends on t since $\alpha(k) = 0$ was excluded as the degenerate case. Hence the convergence of an initial state under the dynamics of the QCA is restricted to states with vanishing first moments.

It is remarkable that while the initial state is a pure, uncorrelated state and the dynamics is reversible for the whole system as well as for every mode, the system exhibits convergence under interplay of the plane-wave modes. However, we only consider observables with finite support on the chain; hence this behavior suggests that correlations are »radiated to infinity« during time evolution. Since the whole range of intermediate states is mapped to the same limit state, the system exhibits the signs of *irreversibility* we are interested in:

Proposition 4.7:
A translationally invariant linear chain of single harmonic oscillators which evolves

- ▷ from a pure Gaussian state with finite correlation length (clustering state) and vanishing first moments
- ▷ under a quasi-free dynamics governed by a nonsqueezing symplectic transformation

reaches a stationary state in the limit of large time.

The limit state of the time evolution is determined by the second, stationary term in (4.25). For all reflection symmetric states, i.e. states with $\gamma(x) = \gamma(-x)$ and thus $\widehat{\gamma}_0(k) = \widehat{\gamma}_0(-k)$ as in our example system, the projection character of P_k and $\overline{P_k}$ effectively reduces $\widehat{\gamma}_0(k)$ to a single matrix element $c(k)$. The limit state is thus described by a single parameter for each mode:

$$\begin{aligned}\gamma_\infty(x) &= \frac{1}{2\pi}\int_{-\pi}^{\pi}\mathrm{d}k\ \mathrm{e}^{\mathrm{i}kx}\left(\left(\overline{P_k}^{\mathrm{T}}\cdot\widehat{\gamma}_0(-k)\cdot P_k\right)^{\mathrm{T}} + \overline{P_k}^{\mathrm{T}}\cdot\widehat{\gamma}_0(k)\cdot P_k\right)\\ &= \frac{1}{2\pi}\int_{-\pi}^{\pi}\mathrm{d}k\ \mathrm{e}^{\mathrm{i}kx}\, c(k)\left(P_k^{\mathrm{T}}\cdot\overline{P_k} + \overline{P_k}^{\mathrm{T}}\cdot P_k\right)\end{aligned} \tag{4.26}$$

Reversing the argument, we can describe any stationary, reflection symmetric state by a unique pure such state and a modewise »temperature« parameter. Casting the expression into a different form gives rise to

Theorem 4.8:
All stationary, translationally invariant and reflection symmetric Gaussian states of the linear chain of single harmonic oscillators with nondegenerate, nearest-neighbor dynamics $\hat{\Gamma}(k)$ from (4.18) are *thermal equilibrium states*, described by their Fourier transformed correlation function $\widehat{\gamma}_{\mathrm{stat}}(k) = g(k)\,\widehat{\varepsilon}(k)$ comprising

- ▷ the correlation function of a pure state with Fourier transform

$$\begin{aligned}\widehat{\varepsilon}(k) &= \mathrm{i}\sigma_{\mathrm{s}}(P_k - \overline{P_k}) \quad \text{for} \quad 0 < \phi < \pi\\ \widehat{\varepsilon}(k) &= \mathrm{i}\sigma_{\mathrm{s}}(\overline{P_k} - P_k) \quad \text{for} \quad -\pi < \phi < 0\end{aligned} \qquad \text{where } \Gamma_0 = \begin{pmatrix}\cos\phi & -\sin\phi\\ \sin\phi & \cos\phi\end{pmatrix}$$

- ▷ and a continuous function $g(k)$ of modewise »temperature« parameters with

$$g(k) = g(-k) \geq 1\,.$$

Proof: The proof is divided into several parts. First, $\hat{\varepsilon}(k)$ is shown to possess the properties claimed in the prelude. Second, $\hat{\varepsilon}(k)$ has to obey the state condition. Third, it corresponds to a pure state and is modified to a mixed state by $g(k)$. And finally, there exists a $g(k)$ such that $g(k)\,\hat{\varepsilon}(k)$ describes the limit state (4.26).

For clarity, the proof is formulated for the case $0 < \phi < \pi$. However, it holds for $-\pi < \phi < 0$ by the same arguments. An exception is made for the state condition of $\hat{\varepsilon}(k)$, where positivity requires consideration of both cases.

Firstly, the Fourier transformed correlation function $\widehat{\varepsilon}(k)$ is indeed symmetric under interchange of k and $-k$ since $\hat{\Gamma}(-k) = \hat{\Gamma}(k)$ by (4.18) as well as $\alpha(-k) = \alpha(k)$ by (4.19) and thus $P_{-k} = P_k$, $\overline{P_{-k}} = \overline{P_k}$ from (4.22). Moreover, $\widehat{\varepsilon}(k)$ is invariant under the dynamics. To see this, note from (4.21) that $\hat{\Gamma}(k)$ commutes with P_k and $\overline{P_k}$ since $P_k\,\overline{P_k} = \overline{P_k}\,P_k = 0$. For a single mode per site, as in our example, $\det \hat{\Gamma}(k) = 1$ by the definition in (4.18) implies that $\hat{\Gamma}(k)$ is a symplectic transformation and thus leaves σ_s invariant. The following equalities then show that $\widehat{\varepsilon}(k)$ does not change under the action of Γ:

$$\hat{\Gamma}^{\mathrm{T}}(k) \cdot \widehat{\varepsilon}(k) \cdot \hat{\Gamma}(k) = \mathrm{i}\,\hat{\Gamma}^{\mathrm{T}}(k)\,\sigma_\mathrm{s}\,\hat{\Gamma}(k) \cdot (P_k - \overline{P_k}) = \mathrm{i}\,\sigma_\mathrm{s}\,(P_k - \overline{P_k}) = \widehat{\varepsilon}(k).$$

In order to see that $\widehat{\varepsilon}(k)$ also fulfills the state condition $\widehat{\varepsilon}(k) + \mathrm{i}\sigma_\mathrm{s} \geq 0$ from Lemma 4.5 consider the identity

$$\widehat{\varepsilon}(k) + \mathrm{i}\sigma_\mathrm{s} = \mathrm{i}\sigma_\mathrm{s} \cdot (P_k - \overline{P_k} + \mathbb{1}) = 2\mathrm{i}\sigma_\mathrm{s}\,P_k\,.$$

Since P_k has rank one, the only nonzero eigenvalue of $\mathrm{i}\sigma_\mathrm{s}\,P_k$ is given by the trace, $\mathrm{tr}[\mathrm{i}\sigma_\mathrm{s}\,P_k] = (\sin\phi - f\cos(k)\cos\phi)/\sin\alpha(k)$. As $\alpha(k)$ is restricted w.l.o.g. to the interval $(0,\pi)$, cf. Lemma 4.6, the denominator is always positive, $\sin\alpha(k) > 0$. By the condition on f from (4.20), the numerator and thus the nonzero eigenvalue is positive for $0 < \phi < \pi$ and negative for $-\pi < \phi < 0$. (Note that we have excluded the degenerate cases with $\phi \in \{0, \pm\pi\}$ for which the numerator is zero.) Hence $\widehat{\varepsilon}(k)$ obeys the state condition with the appropriate differentiation of cases from the statement of the theorem. In addition, $\widehat{\varepsilon}(k)$ corresponds to a pure state since $\big(\sigma_\mathrm{s} \cdot \widehat{\varepsilon}(k)\big)^2 = -\mathbb{1}$. Moreover, $\widehat{\varepsilon}(k)$ can be modified modewise by a factor $g(k) = g(-k) \geq 1$ without affecting the above relations, except for the pure state condition. Hence $g(k)$ plays the role of a »temperature« for the plane-wave modes.

It remains to connect the stationary states $g(k)\,\widehat{\varepsilon}(k)$ to the limit state of Eq. (4.26). This is accomplished by the choice $g(k) = c(k)\,\|\phi_k\|$. Note that $c(k)$ is real-valued and obeys $c(k) = c(-k)$ since $\hat{\gamma}_0(k)$ as well as P_k and $\overline{P_k}$ are reflection symmetric (see beginning of proof). Hence $g(k) = g(-k) \in \mathbb{R}$. The first task is to connect $\mathrm{i}\sigma_\mathrm{s}\,P_k$ with $P_k^*\,P_k$. Since $\hat{\Gamma}(k)$ is a symplectic transformation, expanding the identity $P_k^{\mathrm{T}} \cdot \big(\sigma_\mathrm{s} \cdot P_k\big) = P_k^{\mathrm{T}} \cdot \big(\hat{\Gamma}^{\mathrm{T}}(k)\,\sigma_\mathrm{s}\,\hat{\Gamma}(k) \cdot P_k\big)$ implies $P_k^{\mathrm{T}}\,\sigma_\mathrm{s}\,P_k = 0$ and in turn the relation

$$\mathrm{i}\sigma_\mathrm{s}\,P_k = \mathrm{i}(P_k^{\mathrm{T}} + P_k^*) \cdot \sigma_\mathrm{s}\,P_k = P_k^* \cdot \mathrm{i}\sigma_\mathrm{s} \cdot P_k\,. \tag{4.27}$$

The nonorthogonal projector P_k can be written as $P_k = |\phi_k\rangle\langle\psi_k|$, where we assume w.l.o.g. that $\|\psi_k\| = 1$ while in general $\|\phi_k\| \neq 1$. However, the condition $P_k^2 = P_k$ requires $\langle\psi_k|\phi_k\rangle = 1$. With this, we have $\mathrm{i}\sigma_\mathrm{s}\,P_k = P_k^* \cdot \mathrm{i}\sigma_\mathrm{s} \cdot P_k = r\,|\psi_k\rangle\langle\psi_k|$, where $r = \langle\phi_k|\mathrm{i}\sigma_\mathrm{s}|\phi_k\rangle$. Indeed, r is real-valued since

$$r^2 = \big(\langle\phi_k|\mathrm{i}\sigma_\mathrm{s}|\phi_k\rangle\big)^2 = \langle\phi_k|\mathrm{i}\sigma_\mathrm{s} \cdot P_k\,P_k^* \cdot \mathrm{i}\sigma_\mathrm{s}|\phi_k\rangle = \big|\langle\phi_k|\psi_k\rangle\big|^2\,\|\phi_k\|^2 = \|\phi_k\|^2.$$

So, $\mathrm{i}\sigma_\mathrm{s} P_k = \|\phi_k\| \, |\psi_k\rangle\langle\psi_k|$ (if we assume again that $0 < \phi < \pi$). Compare this with $P_k^* P_k = \|\phi_k\|^2 \, |\psi_k\rangle\langle\psi_k|$ to see that $g(k)\,\mathrm{i}\sigma_\mathrm{s} P_k = c(k) P_k^* P_k$. By complex conjugation, $-g(k)\,\mathrm{i}\sigma_\mathrm{s} \overline{P_k} = c(k) P_k^\mathrm{T} \overline{P_k}$ follows. Moreover, $g(k) = g(-k) = c(k)\,\|\phi_k\|$ is an admissible temperature function, i.e. $c(k)\,\|\phi_k\| \geq 1$ by the following reasoning: Since the correlation function $\gamma_0(x)$ is real, it has to obey two complex conjugated versions of the state condition, $\gamma_0 \pm \mathrm{i}\sigma \geq 0$ (see Section 4.2.1 for a discussion). Similarly, its Fourier transform has to obey $\widehat{\gamma}_0(k) - \mathrm{i}\sigma \geq 0$. Compressing this relation with P_k yields:

$$0 \leq P_k^* \cdot \widehat{\gamma}_0(k) \cdot P_k - P_k^* \cdot \mathrm{i}\sigma \cdot P_k = \big(c(k) - 1/\|\phi_k\|\big)\, P_k^* P_k \,.$$

But since $P_k^* P_k \geq 0$, necessarily $c(k)\,\|\phi_k\| \geq 1$. So, indeed $g(k) = c(k)\,\|\phi_k\| = g(-k) \geq 1$ and $g(k)\,\widehat{\varepsilon}(k)$ is the limit state of (4.26). □

Note that $\widehat{\varepsilon}(k)$ can be expressed in terms of $\hat{\Gamma}(k)$ and $\alpha(k)$ more directly:

$$\widehat{\varepsilon}(k) = \mathrm{i}\sigma_\mathrm{s}(P_k - \overline{P_k}) = -2\sigma_\mathrm{s} \operatorname{Im} P_k = -\sigma_\mathrm{s}\big(\cos\alpha(k)\,\mathbb{1} - \hat{\Gamma}(k)\big)\,\big(\sin\alpha(k)\big)^{-1}. \quad (4.28)$$

Since we excluded the degenerate case with $\sin\alpha(k) = 0$, the matrix elements of $\widehat{\varepsilon}(k)$ are always finite. Moreover, $\widehat{\varepsilon}(k)$ is continuous and hence $\gamma_\infty(x)$ is absolutely summable.

In [3], pointwise convergence of characteristic functions $\chi_n(\xi)$ to $\chi_\infty(\xi)$ was used to establish convergence of the respective density operators ρ_n to ρ_∞ in trace norm. The argument is based on results from [85], where pointwise convergence of $\chi_n(\xi)$ was shown to imply weak convergence of ρ_n, and from [86, 87], showing that weak convergence of density operators is equivalent to convergence in trace norm. Similar reasoning in our case leads to the following result:

Theorem 4.9:
Let ρ_0 be a translationally invariant Gaussian state with reflection symmetric correlation function $\gamma_0(x) = \gamma_0(-x)$, finite correlation length and vanishing first moments. Under the dynamics of a QCA as described, ρ_0 converges to a stationary state ρ_∞ in trace norm *on finite regions of the lattice*. The limit state is described by the correlation function $\gamma_\infty(x)$ from (4.26) and the characteristic function

$$\chi_\infty(\xi) = \exp\Big(-\tfrac{1}{4} \sum_{x,y\in\mathbb{Z}} \xi_x^\mathrm{T} \cdot \gamma_\infty(x-y) \cdot \xi_y\Big). \quad (4.29)$$

Proof: The input state ρ_0 has exactly the properties which are prerequisites in Proposition 4.7. Hence its correlation function $\gamma_0(x)$ evolves to functions $\gamma_t(x)$ from (4.25) and converges pointwise to $\gamma_\infty(x)$ from (4.26). The characteristic functions

$$\chi_t(\xi) = \exp\Big(-\tfrac{1}{4} \sum_{x,y\in\mathbb{Z}} \xi_x^\mathrm{T} \cdot \gamma_t(x-y) \cdot \xi_y\Big)$$

of the intermediate states ρ_t thus converge pointwise to $\chi_\infty(\xi)$ from (4.29). We use the arguments from [85] and [86, 87] to turn this pointwise convergence of characteristic functions first into weak convergence of the ρ_t to ρ_∞ and then to establish

convergence in trace norm, i.e.

$$\|\rho_t - \rho_\infty\|_1 = \mathrm{tr}\big[|\rho_t - \rho_\infty|\big] \to 0 \quad \text{as} \quad t \to \infty\,.$$

Note that the knowledge about the limit state simplifies the proof. Since the characteristic function χ_∞ is continuous, the limit state is indeed described by a density operator ρ_∞. Moreover, $\chi_\infty(0) = 1$ implies $\mathrm{tr}[\rho_\infty] = 1$, cf. Section 2.1.1.

In contrast to the general case considered in [85], we restrict the discussion to expectation values of the ρ_t with operators from the quasi-local algebra $\mathcal{A}(\mathbb{Z})$, which is generated by the Weyl operators with finite support. Therefore, it suffices to assure convergence with respect to these operators. But expectation values with such Weyl operators are exactly the pointwise values of the characteristic function:

$$\mathrm{tr}\big[\rho_\infty\,\mathrm{W}(\xi)\big] = \chi_\infty(\xi) = \lim_{t\to\infty}\chi_t(\xi) = \lim_{t\to\infty}\mathrm{tr}\big[\rho_t\,\mathrm{W}(\xi)\big].$$

This is the statement of weak convergence $\rho_t \xrightarrow{\mathrm{w}} \rho_\infty$ on $\mathcal{A}(\mathbb{Z})$.

To establish convergence in trace norm, we closely follow the proof of Lemma 4.3 in [86], which we provide for completeness: Given $0 < \varepsilon < 1$, let P be a spectral projector for ρ_∞ with finite rank and $\|\rho_\infty - P\rho_\infty P\|_1 < \varepsilon$. By the triangle inequality, we can bound the trace norm distance of any ρ_t and ρ_∞ as

$$\|\rho_\infty - \rho_t\|_1 \leq \|\rho_\infty - P\rho_\infty P\|_1 + \|P\rho_\infty P - P\rho_t P\|_1 + \|P\rho_t P - \rho_t\|_1\,. \tag{4.30}$$

Assuming the spectral decomposition $\rho_t = \sum_{m=1}^\infty r_m |e_m\rangle\langle e_m|$, where $\{|e_m\rangle\}_{m=1}^\infty$ is an orthonormal basis of the Hilbert space, the authors of [86] derive an upper bound for the last term:

$$\begin{aligned}
\|\rho_t - P\rho_t P\|_1 &\leq \|\rho_t - P\rho_t\|_1 + \|P\rho_t - P\rho_t P\|_1 \\
&\leq \sum_{m=1}^\infty r_m \big\||e_m\rangle\langle e_m| - P|e_m\rangle\langle e_m|\big\|_1 + \\
&\qquad \sum_{m=1}^\infty r_m \big\|P|e_m\rangle\langle e_m| - P|e_m\rangle\langle e_m|P\big\|_1 \\
&= 2\sum_{m=1}^\infty r_m \Big(1 - \big\|P|e_m\rangle\big\|_1^2\Big)^{1/2} \\
&\leq 2\left\{\sum_{m=1}^\infty r_m\right\}^{1/2}\left\{\sum_{m=1}^\infty r_m\Big(1 - \big\|P|e_m\rangle\big\|_1^2\Big)\right\}^{1/2} \\
&\leq 2\left\{\mathrm{tr}[\rho_t] - \sum_{m=1}^\infty r_m\big\|P|e_m\rangle\big\|_1^2\right\}^{1/2} \\
&= 2\left\{\mathrm{tr}[\rho_t] - \mathrm{tr}[P\rho_t P]\right\}^{1/2}.
\end{aligned} \tag{4.31}$$

As $\rho_t \xrightarrow{\mathrm{w}} \rho_\infty$, $P\rho_t P$ converges weakly to $P\rho_\infty P$. Since P is of finite rank, there exists a number $T \in \mathbb{N}$ such that for all time steps $t \geq T$ the bound $\|P\rho_t P - P\rho_\infty P\|_1 < \varepsilon^2$

holds. Note that the trace norm bounds also imply bounds on the respective traces:

$$\|A-B\|_1 < \varepsilon^2 \implies \big|\mathrm{tr}[A-B]\big| \leq \mathrm{tr}\big[|A-B|\big] = \|A-B\|_1 < \varepsilon^2.$$

This allows to establish a bound on (4.31) for all $t \geq T$:

$$\begin{aligned}\big|\mathrm{tr}[\rho_t] - \mathrm{tr}[P\rho_t P]\big| &\leq \big|\mathrm{tr}[\rho_t] - \mathrm{tr}[\rho_\infty]\big| + \big|\mathrm{tr}[\rho_\infty] - \mathrm{tr}[P\rho_\infty P]\big| \\ &\qquad + \big|\mathrm{tr}[P\rho_\infty P] - \mathrm{tr}[P\rho_t P]\big| \\ &\leq 0 + \big\|\rho_\infty - P\rho_\infty P\big\|_1 + \big\|P\rho_\infty P - P\rho_t P\big\|_1 \\ &< 2\varepsilon^2,\end{aligned}$$

since $\mathrm{tr}[\rho_t] = \mathrm{tr}[\rho_\infty] = 1$. Hence, by (4.31), $\|\rho_t - P\rho_t P\|_1 < 2\sqrt{2}\,\varepsilon$ and finally from (4.30)

$$\|\rho_\infty - \rho_t\|_1 < \varepsilon^2 + \varepsilon^2 + 2\sqrt{2}\,\varepsilon < 6\varepsilon.$$

This proves convergence of ρ_t and thus of ρ_0 under the dynamics to ρ_∞ in trace norm with respect to finitely localized observables, i.e. finite lattice regions. □

4.3 Irreversible Gaussian QCA

By an irreversible QCA, we understand a QCA with a global rule T which has, however, no completely positive inverse. The dynamics thus cannot be inverted by physical operations. In contrast to the reversible case, irreversible QCAs still resist a detailed characterization. So far, investigations have been restricted to special classes of such systems, e.g. in [88]. In this chapter, we highlight a few problems in the characterization of irreversible QCAs for Gaussian systems.

As mentioned above, several desirable features which come built in for reversible QCAs pose difficulties in the irreversible case. While Definition 4.1 covers the essential properties of a QCA, it does, however, not consider two important principles:

(i) the local rule should determine the global rule (Lemma 4.2) and

(ii) the concatenation of QCAs should again be a QCA (Corollary 4.3).

The first principle allows to explicitly obtain the global rule of a QCA for every valid local dynamics. This complements the axiomatic definition of the class of QCAs with a constructive approach for individual automata. The second property allows to build a QCA out of set of »module« QCAs. In particular, two steps of any given QCA would result in a combined dynamics which again is a (different) QCA. We will in the following investigate how these properties influence the definition of irreversible Gaussian QCAs.

As above, an irreversible Gaussian QCA has a quasi-free dynamics, which maps Weyl operators to multiples of Weyl operators. This is accomplished by a linear transformation Γ of the phase space argument and additional noise to assure complete positivity (cf. Section 2.3). In the reversible case, a symplectic Γ renders

$T\big(\mathrm{W}(\xi)\big) = \mathrm{W}(\Gamma\,\xi)$ an automorphism. Consequentially, for irreversible QCAs Γ must not be symplectic. Instead, the dynamics T is determined by a general linear transformation Γ and an appropriate noise factor which we write as an exponential for convenience, cf. Eq. (2.40):

$$T\big(\mathrm{W}(\xi)\big) = \mathrm{W}(\Gamma\,\xi)\,\mathrm{e}^{-g(\xi,\xi)/4}\,, \tag{4.32}$$

where $g(\xi,\eta)$ is real-valued and symmetric. (As in the reversible case, it suffices to consider T on Weyl operators, cf. Section 4.2.2.) A translationally invariant Gaussian input state with correlation function $\gamma(\xi,\xi)$ and uniform displacement d is transformed into a state with characteristic function

$$\chi(\xi) = \exp\Big(-\gamma(\Gamma\,\xi,\Gamma\,\xi)/4 + g(\xi,\xi)/4 + \mathrm{i}\sum_{x\in\mathbb{Z}}(\Gamma\,\xi)_x^{\mathrm{T}}\cdot d\Big)\,, \tag{4.33}$$

which has again Gaussian shape. Since the dynamics is supposed to be translationally invariant, Γ and g have to be invariant under lattice translations and are thus determined by functions $\Gamma(x)$ and $g(x)$ of the distance x between sites. In addition, to assure a finite propagation speed for compliance with Definition 4.1, Γ has to be restricted to $\mathcal{N}$ by requiring $\Gamma(x) = 0$ for $x \notin \mathcal{N}$. According to Theorem 2.6, T is completely positive if

$$C \equiv g + \mathrm{i}\sigma - \mathrm{i}\Gamma^{\mathrm{T}}\sigma\,\Gamma \geq 0 \tag{4.34}$$

in the sense of (4.5). As an aside, note that this condition allows for two special solutions:

- ▷ Γ is symplectic: This corresponds to a reversible QCA with classical Gaussian excess noise determined by $g \geq 0$.
- ▷ $\Gamma = 0$: The resulting QCA immediately discards its input and replaces it by a translationally invariant Gaussian state with covariance matrix g, which is admissible since (4.34) reduces to the state condition $g + \mathrm{i}\sigma \geq 0$. This completely depolarizing dynamics has a classical analog for product states, where the CA locally replaces the state of every cell by a uniform standard value.

The dynamics described above conforms to Definition 4.1, but does not necessarily incorporate the extensions (i) and (ii) from above. To see this, consider the outcome of T for a product of Weyl operators:

$$\begin{aligned} T\big(\mathrm{W}(\xi)\,\mathrm{W}(\eta)\big) &= \exp\big(-\mathrm{i}\sigma(\xi,\eta)/2\big)\,T\big(\mathrm{W}(\xi+\eta)\big) \\ &= \exp\big(-\mathrm{i}\sigma(\xi,\eta)/2 - g(\xi+\eta,\xi+\eta)/4\big)\ \mathrm{W}(\Gamma\,\xi+\Gamma\,\eta) \\ &= \exp\big(\mathrm{i}\sigma(\Gamma\,\xi,\Gamma\,\eta)/2 - \mathrm{i}\sigma(\xi,\eta)/2 - g(\xi,\eta)/2\big) \\ &\qquad \mathrm{e}^{-g(\xi,\xi)/4}\ \mathrm{W}(\Gamma\,\xi)\,\mathrm{e}^{-g(\eta,\eta)/4}\ \mathrm{W}(\Gamma\,\eta) \end{aligned}$$

and hence

$$T\big(\mathrm{W}(\xi)\,\mathrm{W}(\eta)\big) = \mathrm{e}^{-C(\xi,\eta)/2}\,T\big(\mathrm{W}(\xi)\big)\,T\big(\mathrm{W}(\eta)\big). \tag{4.35}$$

(Recall that g is symmetric and $C = g + \mathrm{i}\sigma - \mathrm{i}\Gamma^{\mathrm{T}}\,\sigma\,\Gamma$ from (4.34).) The couplings introduced by the dissipation form C spoil the connection between local and global rule for property (i), since unlike in the proof of Lemma 4.2, $T(A)$ for an arbitrary localized observable A cannot be solely expressed in terms of single-site constituents. This problem can in principle be overcome by imposing additional conditions on C and thus on Γ and g. However, it is not immediately clear what requirements correspond to properties (i) and (ii).

As a first step towards a resolution of this issue, we distinguish between different notions of »localization« which are relevant for general, not necessarily Gaussian irreversible QCAs. These are connected to different neighborhoods (which we again w.l.o.g. assume to contain the origin):

I. Finite propagation speed with neighborhood scheme $\mathcal{N}$: Observables which are localized on a finite region Λ of the lattice are mapped to observables localized on $\Lambda + \mathcal{N}$,

$$T\big(\mathcal{A}(\Lambda)\big) \subset \mathcal{A}(\Lambda + \mathcal{N}).$$

II. Factorization with respect to a symmetric $\mathcal{M}$, i.e. $\mathcal{M} = -\mathcal{M}$: A tensor product of observables $A_1 \in \mathcal{A}(\Lambda_1)$ and $A_2 \in \mathcal{A}(\Lambda_2)$ on disjoint, finite regions Λ_1 and Λ_2 which are separated by $\mathcal{M}$, i.e. $(\Lambda_1 + \mathcal{M}) \cap \Lambda_2 = \emptyset$, is mapped to a product,

$$T(A_1 \otimes A_2) = T(A_1)\,T(A_2).$$

III. Localization of Kraus operators on $\mathcal{K}$: For any finite region Λ there exists a finite set of Kraus operators localized on $\Lambda + \mathcal{K}$ which implement the dynamics,

$$\forall \Lambda\ \exists \big\{ K_i \mid K_i = K_i(\Lambda) \in \mathcal{A}(\Lambda + \mathcal{K}) \big\}\ \forall A \in \mathcal{A}(\Lambda)\colon\ T(A) = \sum\nolimits_i K_i^* A\, K_i\,.$$

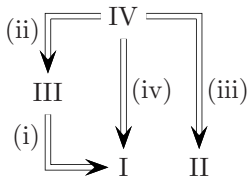
IV. Local dilation on $\mathcal{D}$: The dynamics consists of three steps. First, in the Schrödinger picture, for each cell a local ancilla system is prepared in a fixed state ρ_0. Second, a reversible QCA given by an automorphism T_1 with neighborhood scheme $\mathcal{D}$ is run on the extended system. And third, at each site the ancilla system is traced out. Denote the algebra of the ancilla system by $\mathcal{E}$ and the respective quasi-local algebra for the whole lattice by $\mathcal{E}(\mathbb{Z}^s)$. If $\mathcal{A}'(\mathbb{Z}^s)$ is the tensor product $\mathcal{A}(\mathbb{Z}^s) \otimes \mathcal{E}(\mathbb{Z}^s)$ and $\mathrm{tr}_{\mathcal{E}}$ is the trace over the ancilla systems, then

$$\begin{aligned}
&T_1\colon \mathcal{A}'(\mathbb{Z}^s) \to \mathcal{A}'(\mathbb{Z}^s) \text{ automorphism with } T_1\big(\mathcal{A}'(\Lambda)\big) \subset \mathcal{A}'(\Lambda + \mathcal{D}),\\
&T_*(\rho) = \mathrm{tr}_{\mathcal{E}}\big[T_{1*}(\rho \otimes \rho_0^{\otimes \mathbb{Z}^s})\big] \text{ in the Schrödinger picture and}\\
&T(A) = \mathrm{tr}_{\mathcal{E}}\big[\mathbb{1} \otimes \rho_0^{\otimes \mathbb{Z}^s}\, T_1(A \otimes \mathbb{1})\big] \text{ in the Heisenberg picture.}
\end{aligned}$$

Note that every system which is a QCA by Definition 4.1 falls into category I. In addition, II has to hold with $\mathcal{N} - \mathcal{N} \subseteq \mathcal{M}$ in order to assure causality.[9] In order to establish which conditions should be imposed to guarantee the desired properties, consider connections between the cases:

Lemma 4.10:
The above notions of locality constitute a partial hierarchy in the sense that

(i) III implies I with $\mathcal{N} = \mathcal{K}$,
(ii) IV implies III with $\mathcal{K} = \mathcal{D}$,
(iii) IV implies II with $\mathcal{M} = \mathcal{D} - \mathcal{D}$,
(iv) IV implies I with $\mathcal{N} = \mathcal{D}$.
(v) However, II does not imply I and vice versa.



Remark: It remains open if any of the lower cases imply higher ones, e.g. if I and II together already require IV.

Proof:

(i) By the embedding described in Section 4.1, $A \in \mathcal{A}(\Lambda)$ is also in $\mathcal{A}(\Lambda + \mathcal{K})$. Since $K_i \in \mathcal{A}(\Lambda + \mathcal{K})$, obviously $T(A) = \sum_i K_i^* A K_i \in \mathcal{A}(\Lambda + \mathcal{K})$ and hence $T\big(\mathcal{A}(\Lambda)\big) \subset \mathcal{A}(\Lambda + \mathcal{K})$.

(ii) As every channel, the dynamics of IV can be described by Kraus operators, see Section 2.3. For $A \in \mathcal{A}(\Lambda)$, we have by definition $T_1(A) \in \mathcal{A}'(\Lambda + \mathcal{D})$ and $T(A) = \mathcal{A}(\Lambda + \mathcal{D})$ since the ancilla systems do not introduce correlations. Hence $K_i \in \mathcal{A}(\Lambda + \mathcal{D})$.

(iii) For $A_1 \in \mathcal{A}(\Lambda_1)$, $A_2 \in \mathcal{A}(\Lambda_2)$ and $(\Lambda_1 + \mathcal{D}) \cap (\Lambda_2 + \mathcal{D}) = \emptyset$, the observables $T_1(A_1)$ and $T_1(A_2)$ are localized on different regions $\mathcal{A}'(\Lambda_1 + \mathcal{D})$ and $\mathcal{A}'(\Lambda_2 + \mathcal{D})$ without overlap. Hence their product can be written as a tensor product with respect to the sites by implicit embedding. Since T_1 is an automorphism, this yields:

$$\begin{aligned} T(A_1\, A_2) &= \mathrm{tr}_{\mathcal{E}}\big[\mathbb{1} \otimes \rho_0^{\otimes \mathbb{Z}^s}\, T_1(A_1 \otimes \mathbb{1})\, T_1(A_2 \otimes \mathbb{1})\big] \\ &= \mathrm{tr}_{\mathcal{E}}\big[\mathbb{1} \otimes \rho_0^{\otimes (\Lambda_1 + \mathcal{D})}\, T_1(A_1 \otimes \mathbb{1})\big]\ \mathrm{tr}_{\mathcal{E}}\big[\mathbb{1} \otimes \rho_0^{\otimes (\Lambda_2 + \mathcal{D})}\, T_1(A_2 \otimes \mathbb{1})\big] \\ &= T(A_1)\, T(A_2). \end{aligned}$$

9 Note that $(\Lambda_1 + \mathcal{D} - \mathcal{D}) \cap \Lambda_2 = \emptyset \iff (\Lambda_1 + \mathcal{D}) \cap (\Lambda_2 + \mathcal{D}) = \emptyset$. Causality is the notion that operations on sufficiently far separated areas should be independent of each other. In our terms, this requires for observables $A_1 \in \mathcal{A}(\Lambda_1)$ and $A_2 \in \mathcal{A}(\Lambda_2)$, where $T(A_i) \in \mathcal{A}(\Lambda_i + \mathcal{N})$ and $(\Lambda_1 + \mathcal{N}) \cap (\Lambda_2 + \mathcal{N}) = \emptyset$ that

$$\begin{aligned} T(A_1 \otimes \mathbb{1}|_{\Lambda_2 + \mathcal{N}}) &= T(A_1) \otimes \mathbb{1}|_{\Lambda_2 + \mathcal{N}}, \\ T(\mathbb{1}|_{\Lambda_1 + \mathcal{N}} \otimes A_2) &= \mathbb{1}|_{\Lambda_1 + \mathcal{N}} \otimes T(A_2). \end{aligned}$$

(For details and a brief discussion, see e.g. [89].) Note that under this conditions in II we get $T(A_1 \otimes A_2) = T(A_1)\, T(A_2) = T(A_1) \otimes T(A_2)$ by implicit embedding.

Note that the tensor products above are with respect to the decomposition of main system and ancilla at each site.

(iv) This follows from (ii) and (i).

(v) Consider a dynamics which completely depolarizes an initial state ρ_{in} to a translationally invariant product state $\rho_0^{\bigotimes \mathbb{Z}^s}$. For $A_1 \in \mathcal{A}(\Lambda_1)$, $A_2 \in \mathcal{A}(\Lambda_2)$ and $(\Lambda_1 + \mathcal{M}) \cap \Lambda_2 = \emptyset$ we get

$$\operatorname{tr}\bigl[\rho_{\text{in}}\, T(A_1 \otimes A_2)\bigr] = \operatorname{tr}\bigl[\rho_0^{\bigotimes \Lambda_1} A_1\bigr]\, \operatorname{tr}\bigl[\rho_0^{\bigotimes \Lambda_2} A_2\bigr] = \operatorname{tr}\bigl[\rho_{\text{in}}\, T(A_1)\bigr]\, \operatorname{tr}\bigl[\rho_{\text{in}}\, T(A_2)\bigr].$$

Hence $T(A_1 \otimes A_2) = T(A_1)\, T(A_2)$ and II holds true independently of I and $\mathcal{M}$ (as long as $0 \in \mathcal{M}$). For the converse, the Gaussian dynamics from (4.32) serves as a counterexample by virtue of (4.35) if $g(x)$ is not restricted to a *finite* $\mathcal{M}$. □

For Gaussian irreversible QCAs, the cases I and II are easily expressed in terms of Γ and g:

Lemma 4.11:
A Gaussian irreversible QCA, described by dynamics Γ and noise form g, complies with type I or II, respectively, if

I. $\Gamma(x) = 0$ for $x \notin \mathcal{N}$,

II. $g(x) = 0$ for $x \notin \mathcal{M}$ and

$$\forall \Delta \in (\mathcal{N} - \mathcal{N}) \setminus \mathcal{M} \colon \sum_{x \in \mathcal{N}} \Gamma_x^+ \, \Gamma_{\Delta + x} = 0\,. \tag{4.36}$$

Remark: If $\mathcal{N} - \mathcal{N} \subseteq \mathcal{M}$, case II does not impose a condition on Γ. Otherwise, (4.36) corresponds to part of the condition (4.10) for Γ to be symplectic. Consider in particular the important case $\mathcal{M} = \{0\}$; as for reversible QCAs, this allows to reconstruct the global rule from the local rule by the arguments from the proof of Lemma 4.2. For a nearest-neighbor interaction, in detail Γ has to obey the conditions (4.11b–e) but not (4.11a). Hence for systems with one mode per site a deviation from symplectic transformations is possible by choosing e.g. $\Gamma_0^+ \Gamma_0 \neq \mathbb{1}$.

Proof: Compliance with case I was already considered above and corresponds to finite support for Γ, i.e. $\Gamma(x) = 0$ for $x \notin \mathcal{N}$. For case II to apply, the dissipation form C from (4.34) has to vanish due to (4.35) if the supports $\operatorname{supp}\xi$ and $\operatorname{supp}\eta$ are separated by $\mathcal{M}$,

$$(\operatorname{supp}\xi + \mathcal{M}) \cap \operatorname{supp}\eta = \emptyset \implies C(\xi, \eta) = g(\xi, \eta) + \mathrm{i}\sigma(\xi, \eta) - \mathrm{i}\sigma(\Gamma^{\mathrm{T}}\xi, \Gamma\,\eta) = 0\,.$$

Since we assume $0 \in \mathcal{M}$, this implies $\operatorname{supp}\xi \cap \operatorname{supp}\eta = \emptyset$ and $\sigma(\xi, \eta) \equiv 0$. As Γ and g are real-valued, the condition can be split into real and imaginary parts

$$g(\xi, \eta) = 0 \quad \text{and} \quad \sigma(\Gamma^{\mathrm{T}}\xi, \Gamma\,\eta) = 0\,, \tag{4.37}$$

respectively, which have to hold true independently of each other. Hence require $g(x) = 0$ for $x \notin \mathcal{M}$. Recall that for causality, $g(x) = 0$ for $x \notin \mathcal{N} - \mathcal{N}$ is necessary in any case, see above. If $\mathcal{N} - \mathcal{N} \subseteq \mathcal{M}$, even $\sigma(\Gamma^{\mathrm{T}}\,\xi, \Gamma\,\eta) \equiv 0$ and the condition is satisfied independently of Γ. Otherwise, however, (4.37) imposes restrictions on Γ also, which are obtained in the same way as for (4.10):

$$\forall \Delta \in (\mathcal{N} - \mathcal{N}) \setminus \mathcal{M} \colon \sum_{x \in \mathcal{N}} \Gamma_x^+ \, \Gamma_{\Delta + x} = 0\,. \tag{4.38}$$

□

While the combination »I+II« of cases I and II with $\mathcal{M} = \{0\}$ thus assures that the global rule can be inferred from the local rule, a concatenation of two such systems is in general not of this type. Hence they comply with property (i), but not with (ii). The concatenation of two channels T_1 and T_2 from (4.32) determined by transformations $\Gamma_i(x)$ with support on $\mathcal{N}_i$ and noise forms $g_i(x)$ with support on $\mathcal{M}_i$ for $i = 1, 2$ results in a combined dynamics T according to

$$\begin{aligned} T\big(\mathrm{W}(\xi)\big) &= T_2\big(T_1(\mathrm{W}(\xi))\big) = \mathrm{W}(\Gamma_2\,\Gamma_1\,\xi)\, \exp\!\big(-g_2(\Gamma_1\,\xi, \Gamma_1\,\xi)/4 - g_1(\xi,\xi)/4\big) \\ &= \mathrm{W}(\Gamma\,\xi)\, \exp\!\big(-g(\xi,\xi)/4\big), \text{ where } \Gamma = \Gamma_2\,\Gamma_1 \text{ and } g = g_1 + \Gamma_1^{\mathrm{T}}\, g_2\, \Gamma_1\,. \end{aligned}$$

The support of Γ and g can be found from the respective translationally invariant functions:

$$\begin{aligned} (\Gamma_2\,\Gamma_1)(x) = \sum_{z \in \mathbb{Z}} \Gamma_2(x - z) \cdot \Gamma_1(z) \quad &\Longrightarrow \mathcal{N} = \mathcal{N}_1 + \mathcal{N}_2\,, \\ g(x) = g_1(x) + \sum_{y,z \in \mathbb{Z}} \Gamma_1^{\mathrm{T}}(y - x) \cdot g_2(y - z) \cdot \Gamma_1(z) \\ &\Longrightarrow \mathcal{M} = \mathcal{M}_1 \cup (\mathcal{M}_2 + \mathcal{N}_1 - \mathcal{N}_1)\,. \end{aligned}$$

This implies that two systems of type I+II with $\mathcal{M}_i = \mathcal{N}_i - \mathcal{N}_i$ *can* be concatenated to yield a system with the same characteristics since $\mathcal{M} = (\mathcal{N}_1 + \mathcal{N}_2) - (\mathcal{N}_1 + \mathcal{N}_2)$. However, for $\mathcal{M}_i = \{0\}$ an additional condition on g_2 is necessary. In this case, $g_i(x) = \delta(x)\, g_i(0)$ due to the restricted support of g_i. Hence

$$\begin{aligned} g(x) &= \delta(x)\, g_1(0) + \sum_{y,z \in \mathbb{Z}} \Gamma_1^{\mathrm{T}}(y - x) \cdot \delta(y - z)\, g_2(0) \cdot \Gamma_1(z) \\ &= \delta(x)\, g_1(0) + \sum_{y \in \mathbb{Z}} \Gamma_1^{\mathrm{T}}(y - x) \cdot g_2(0) \cdot \Gamma_1(y)\,. \end{aligned}$$

To get $g(x) = \delta(x)\, g(0)$, we need

$$\sum_{y \in \mathbb{Z}} \Gamma_1^{\mathrm{T}}(y - x) \cdot g_2(0) \cdot \Gamma_1(y) = \delta(x)\, g_2'(0) \tag{4.39}$$

with a suitable $g_2'(0)$ such that g and Γ obey the condition (4.34). However, there exist systems of type I+II with $\mathcal{M} = \{0\}$ which cannot meet this condition. As a

simple and relevant example, consider the reversible QCA from Section 4.2.4 plus uncorrelated noise and concatenate two steps of this dynamics. It turns out on inspection that the noise form g_2 does not fulfill the condition (4.39) if the coupling constant f is nonzero.

For QCAs of type IV, concatenation is possible by design; since the ancilla systems are used locally, concatenation concerns only the reversible part T_1. Unfortunately, we do not have a complete characterization of all Gaussian QCAs of this type. However, if the reversible QCA and the ancilla state are Gaussian, the irreversible QCA is Gaussian, too, and its parameters can be derived easily. Consider a linear chain of n modes per site plus local ancilla systems with m modes each. We write the translationally invariant symplectic transformation S which determines T_1 according to (4.7) in block decomposition as

$$S_x = \begin{pmatrix} A_x & B_x \\ C_x & D_x \end{pmatrix} \implies \hat{S}(k) = \begin{pmatrix} \hat{A}(k) & \hat{B}(k) \\ \hat{C}(k) & \hat{D}(k) \end{pmatrix},$$

where A_x, $\hat{A}_k$ are $2n \times 2n$ matrices, D_x, $\hat{D}(k)$ have dimension $2m \times 2m$ and B_x, $\hat{B}(k)$, C_x^{T}, $\hat{C}^{\mathrm{T}}(k)$ are $2m \times 2n$ matrices. For the on-site part S_0, A acts on the chain site, D on the ancilla system and B, C introduce local correlations between both. The correlation function of the product state of the ancilla systems is $\gamma'_x = \delta(x)\,\gamma'_0$, which is a real, symmetric $2m \times 2m$ matrix. Then the following holds:

Lemma 4.12:
A reversible Gaussian QCA with dynamics T_1 on $n + m$ modes together with a fixed Gaussian state for all ancilla systems implements an irreversible Gaussian QCA T of type IV. In particular, with the above notation, T is determined by a linear transformation Γ and a noise form g according to (4.32) which have Fourier transforms

$$\widehat{\Gamma}(k) = \hat{A}(k) \quad \text{and} \quad \hat{g}(k) = \overline{\hat{C}^{\mathrm{T}}}(k)\,\hat{\gamma}'(k)\,\hat{C}(k).$$

Proof: The reversible Gaussian QCA T_1 acts on Weyl operators according to (4.7) by applying a translationally invariant symplectic transformation S to the phase space argument,

$$T_1(\mathrm{W}_\xi) = \mathrm{W}_{S\,\xi}\ .$$

The overall dynamics T of the irreversible QCA attaches to each cell an ancilla system in state ρ_0 with correlation function γ' and transforms the combined correlation function $\gamma_x \oplus \gamma'_x$ with S:

$$\gamma_x \mapsto \sum_{y,z\in\mathbb{Z}} \left[S_y^{\mathrm{T}} \cdot (\gamma_z \oplus \gamma'_z) \cdot S_{x-y+z}\right]_{11},$$

where $[M]_{11}$ is the upper left block with dimensions $2n \times 2n$ for a $2(n+m) \times 2(n+m)$ matrix M. Under Fourier transform, the mapping is

$$\hat{\gamma}(k) \mapsto \left[\overline{\hat{S}^{\mathrm{T}}}(k) \cdot \big(\hat{\gamma}(k) \oplus \hat{\gamma}'(k)\big) \cdot \hat{S}(k)\right]_{11}.$$

After carrying out the reduction, this becomes

$$\hat{\gamma}(k) \mapsto \overline{\hat{A}^{\mathrm{T}}}(k) \cdot \hat{\gamma}(k) \cdot \hat{A}(k) + \overline{\hat{C}^{\mathrm{T}}}(k) \cdot \hat{\gamma}'(k) \cdot \hat{C}(k). \tag{4.40}$$

The output state of an irreversible Gaussian QCA with transformation Γ and noise form g is given in (4.33) and corresponds to a transformation of the correlation function as

$$\hat{\gamma}(k) \mapsto \overline{\widehat{\Gamma}^{\mathrm{T}}}(k) \cdot \hat{\gamma}(k) \cdot \widehat{\Gamma}(k) + \hat{g}(k). \tag{4.41}$$

Comparing (4.40) and (4.41) yields for the irreversible QCA T:

$$\widehat{\Gamma}(k) = \hat{A}(k) \quad \text{and} \quad \hat{g}(k) = \overline{\hat{C}^{\mathrm{T}}}(k)\, \hat{\gamma}'(k)\, \hat{C}(k).$$

Indeed, g is real and symmetric as required, i.e. $\hat{g}(k) = -\overline{\hat{g}(-k)} = \overline{\hat{g}(k)}$, because C is real and γ' is real and symmetric. □

So, while reversible Gaussian QCAs with local ancillas can implement irreversible Gaussian QCAs of type IV, the converse is unfortunately not clear: are all irreversible Gaussian QCAs of type IV? The answer to this question is an important step towards the definition of Gaussian as well as general irreversible QCAs.

Private Quantum Channels

5 Gaussian private quantum channels

A private quantum channel is a quantum analog of the classical one-time pad encryption[1] or Vernam cipher: it uses a classical random key to encrypt quantum information. This private information can be exchanged over a public quantum channel if an eavesdropper is not able to extract information from the transmitted states. This is true if the output states of the encryption scheme resemble a randomized state which can only be decrypted if the classical key is known. Besides providing a cryptographic primitive, private quantum channels are, according to [94], conceptually connected with LOCC data hiding, locking of classical correlations and remote state preparation.

To encrypt the i-th input state in a sequence, the sender, conventionally called Alice, applies a unitary operation chosen from a publicly known, finite set $\mathcal{E} = \{U_k\}_{k=1,2,\ldots,K}$ according to the i-th element of the key sequence $\{k_i\}_{i=1,2,\ldots}$ labeling the operations. The resulting state $U_{k_i}\rho U_{k_i}^*$ is sent to the receiver, Bob, who applies the inverse transformation $U_{k_i}^*$ to recover ρ. The only additional information possibly needed for decryption is the position i in the key sequence which could be safely sent in plain text along with the encrypted quantum state. Each element of the key sequence is used only once, hence the protocol resembles the classical one-time pad for quantum states. For an eavesdropper, called Eve, without knowledge about the key, the encryption appears to be a randomization of ρ with respect to the set $\mathcal{E}$, i.e. the channel T from Alice to Eve in the Schrödinger picture is a »shuffle« applied to the input state,

$$T(\rho) = \sum_{k=1}^{K} p_k\, U_k \rho\, U_k^* \,,$$

where p_k denotes the a priori frequencies of the label k in the key sequence. If Eve cannot distinguish the output of T for different input states, the protocol is secure. Apart from an explicit construction of the set of encryptions $\mathcal{E}$ it is interesting to determine the number of operations U_k needed to encrypt a certain set of input states. The binary logarithm of this gives the number of classical bits needed to encrypt e.g. a qubit. Relaxing the security condition to an arbitrarily small distinguishability $\epsilon > 0$ (to be defined below) can significantly lower the number of operations needed.

For finite-dimensional quantum systems, these questions have been addressed e.g. in [90, 91, 92, 93]. In particular, for the ideal encryption of d-level systems a number of d^2 unitaries is necessary and sufficient to completely randomize any input state, i.e. to map it to the maximally mixed state $\mathbb{1}/d$. Furthermore, Hayden et al.

1 In this scheme a classical message is encrypted with a random key of the same length (by combining both sequences bit for bit with the »exclusive or« operation XOR). If the key is truly random and used only once, the cipher is unbreakable.

have shown in [94] that near-perfect encryption can be achieved with order of $d \log d$ random unitary operations.[2] These results have been complemented in [95] by Ambainis and Smith with a deterministic protocol. An investigation of private quantum channels for continuous-variable systems has been started in [96]. Contrary to the finite-dimensional case there is no ideal encryption due to the lack of a maximally mixed state, so one has to rely on approximate encryption. Our aim is to rigorously perform the related discussion for the encryption of coherent input states where the unitary operations are shifts in phase space occurring with probabilities according to a classical Gaussian weight function. On the one hand, the Gaussian weight function renders the channel T between Alice and Eve quasi-free and the randomized states are Gaussian, too. On the other hand, this weight function assures that the twirl[3] over the noncompact group of all phase space translations exists in the first place. This randomization introduces classical noise which can be made large enough to render two coherent input states arbitrarily indistinguishable by inducing a substantial overlap between the resulting output states; see Fig. 5.1 for illustration. As a measure of indistinguishability, we choose the trace norm[4] distance of the output states at Eve's end of the channel, $\|T(\rho) - T(\rho')\|_1$. This quantity has the advantage of an operational meaning since it equals the maximal difference in expectation values of any measurement performed on these states [1].

However, this scheme has several inherent problems. First, the amount of noise to be added depends on the input state; heuristically, the larger its amplitude, the larger the variance of the Gaussian weight function has to be. To keep the protocol as general as possible, this requires a bound on the amplitude of the input coherent states $|\alpha\rangle\langle\alpha|$, i.e. a bound on their occupation number expectation value and hence on their energy[5] $E = |\alpha|^2/2 \leq E_{\max}$. Second, encryption with a continuous set of phase space displacements would require an infinite key for each input state in order to specify the phase space vector precisely. This problem can be overcome by restricting the continuous integral for randomization to a finite area of phase space, e.g. to a hypersphere with radius a, and approximating it with a finite sum over a discrete set of displacements. Finally, since the encryption is only near-perfect, the output state might be distinguishable up to a security parameter ϵ. A general choice for the protocol with approximate security is whether it should be a »block«

2 If output states are required to differ by at most $\epsilon > 0$ in trace norm distance, approximately $(d \log d)/\epsilon^2$ unitaries are needed. The operators can be chosen randomly, since the proof shows that almost any such set of encryption operations yields the desired security.

3 A twirl is the averaging over all elements of a group, i.e. in our case the phase space displacements,

$$\int \mathrm{d}\xi \, \mathrm{e}^{-\xi^{\mathrm{T}} \cdot G \cdot \xi/4} \, \mathrm{W}_\xi \, \rho \, \mathrm{W}_\xi^* \; .$$

4 The trace norm $\|X\|_1$ of an operator X is defined as $\|X\|_1 = \mathrm{tr}|X|$ where $|X| = \sqrt{X^* X}$ is the modulus of X.

5 The energy contained in a mode in a state ρ equals the occupation number expectation value in that state scaled with the characteristic energy of $\hbar\omega$ of the associated harmonic oscillator with frequency ω. We assume that the frequencies of all modes are the same. This would be the case if all modes originate from the same laser mode, but states of this mode might be distinguished e.g. by their temporal ordering.

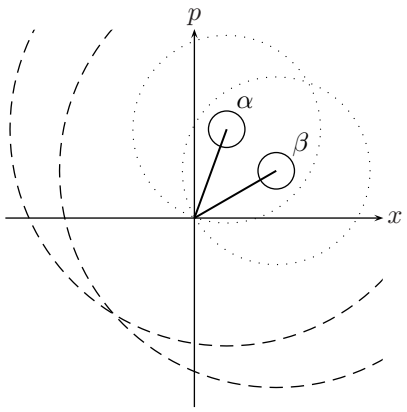


Figure 5.1:
Illustrating the encryption of single-mode coherent states. Two coherent states $|\alpha\rangle\langle\alpha|$ and $|\beta\rangle\langle\beta|$, described by their amplitudes and minimum uncertainty quantum noise and depicted as »lollipop sticks«, are effectively encrypted by adding isotropic classical Gaussian noise. This enlarges the uncertainty from the small circle for $\gamma = \mathbb{1}$ (solid line) to medium and large noise with $\gamma > \mathbb{1}$ (dotted line) and $\gamma \gg \mathbb{1}$ (dashed line), respectively. With growing overlap area of the uncertainty disks, the states become less distinguishable.

or a »stream« cipher, i.e. whether to encrypt blocks of input states or each input state individually, possibly with additional classical correlations between consecutive states. We consider individual encryption but require that the protocol conceals correlations spanning N input states. This includes attacks on the protocol in which Eve performs joint quantum operations on blocks of N output states.

Our task is hence to determine the required key length for a private quantum channel encrypting coherent states with correlations over N input states and maximum energy expectation value $E_{\max}$ such that any two output states at Eve's end differ by at most ϵ in trace norm distance. All other parameters will be fixed accordingly. To assess the security of the protocol, we do not restrict the operations Eve is allowed to perform. However, we assume that she has access only to the transmitted states, neither to the classical key nor to Alice's or Bob's systems or to the original input states.

A quantum device operating according to this scheme could be useful as a building block of a distributed quantum computer using Gaussian quantum systems, e.g. a laser mode, for the transmission of quantum information. Our version of the protocol requires only generic resources (public quantum channel and classical, discrete random key sequence) and does not make particular assumptions about the input states. (While the quantitative security promise requires the knowledge of global parameters about the input states, their values can be arbitrary and thus do not impose restrictions on the set of input coherent states.) It also does not rely on block encoding and can thus send each input state as it arrives. In this sense, the device

would be modular and could be readily attached to the computing units. In addition, our encryption operations are deterministic and implicitly defined, reducing the communication overhead needed to establish the protocol.

We start by formally setting up the continuous encryption as well as cutoff and discrete approximations as quantum channels. After proving the principal security of the continuous encryption, we estimate the precision of the key for the discrete scheme. For correlated multi-mode coherent input states the result can be obtained only implicitly. This is made explicit for independent one-mode coherent states.

The material presented in this chapter is currently being prepared for publication [c]. We would like to thank Kamil Brádler for bringing the topic to our attention as well as for stimulating discussion.

5.1 Setup

This section defines the encryption scheme with continuous displacement formally and introduces its discrete approximation. The security proof will be given in the next section. In the following, all channels will be considered in the Schrödinger picture, i.e. operating on states rather than observables. However, we will customarily write $T(\rho)$ without a star at the index position of T.

To encode an input quantum state ρ, Alice chooses the phase space displacement vector ξ_k matching the first unused element from the key sequence $\{k_i\}_{i=1,2,\dots}$ and applies the corresponding shift to get $\mathrm{W}_{\xi_k}\,\rho\,\mathrm{W}_{\xi_k}^*$, which she sends to Bob over a public quantum channel. Bob can reverse the encoding by applying the inverse shift $-\xi_k$. A vector ξ is supposed to occur with probability $\exp\bigl(-\xi^{\mathrm{T}}\cdot G\cdot\xi/4\bigr)$ in the key sequence, where $G\geq 0$ is the classical covariance matrix of the Gaussian distribution. If Eve has no further knowledge about the sequence, a state $T(\rho)$ she might intercept appears to her as a classical mixture of all possible displacements of the input state, weighted with the Gaussian distribution. The protocol should be secured against collective attacks on blocks of N states. Hence we consider the randomized output $T(\rho)$ of a tensor product of N input coherent states of f modes each,

$$T(\rho)=\frac{1}{c}\int\mathrm{d}\xi\;\mathrm{e}^{-\xi^{\mathrm{T}}\cdot G\cdot\xi/4}\;\mathrm{W}_\xi\,\rho\,\mathrm{W}_\xi^*\,, \tag{5.1}$$

where ξ is understood to be a phase space vector of Nf modes, and the normalization constant c assures that $\mathrm{tr}\bigl[T(\rho)\bigr]=\mathrm{tr}[\rho]$:

$$c=\int\mathrm{d}\xi\;\mathrm{e}^{-\xi^{\mathrm{T}}\cdot G\cdot\xi/4}=(4\pi)^{Nf}/\sqrt{\det G}\,.$$

Classical correlations introduced by Alice between consecutive input states are described by a classical covariance matrix $G\geq 0$ with nonzero off-diagonal blocks. However, for this first analysis, we will not consider the effect of such correlations, but take $G=\mathbb{1}/g$ with $g\gg 1$. The randomized state $T(\rho)$ is described by its

characteristic function

$$\begin{aligned}\chi_{\mathrm{rand}}(\xi) &= \mathrm{tr}\big[T(\rho)\,\mathrm{W}_\xi\big] = \frac{1}{c}\int \mathrm{d}\eta\; \mathrm{e}^{-\eta^{\mathrm{T}}\cdot G\cdot\eta/4}\;\mathrm{tr}\big[\mathrm{W}_\eta\,\rho\,\mathrm{W}_\eta^*\,\mathrm{W}_\xi\big]\\ &= \frac{1}{c}\int \mathrm{d}\eta\; \mathrm{e}^{-\eta^{\mathrm{T}}\cdot G\cdot\eta/4}\,\mathrm{e}^{\mathrm{i}\sigma(\eta,\xi)}\;\chi_{\mathrm{in}}(\xi)\\ &= \exp\big(-\xi^{\mathrm{T}}\cdot(\sigma^{\mathrm{T}}\,G^{-1}\,\sigma)\cdot\xi/4\big)\;\chi_{\mathrm{in}}(\xi).\end{aligned}$$

In the Heisenberg picture, T maps Weyl operators to multiples of themselves, so it is a completely positive map: $\mathrm{W}_\xi \mapsto \mathrm{W}_\xi\,\exp\big(-\xi^{\mathrm{T}}\cdot(\sigma^{\mathrm{T}}\,G^{-1}\,\sigma)\cdot\xi/4\big)$, where $\sigma^{\mathrm{T}}\,G^{-1}\,\sigma \geq 0$ (cf. Section 2.3). Since the factor c assures normalization, it is even a channel. A Gaussian input state with covariance matrix γ and displacement α is transformed into a Gaussian state with characteristic function

$$\chi_{\mathrm{rand}}(\xi) = \exp\big(-\xi^{\mathrm{T}}\cdot(\gamma+\sigma^{\mathrm{T}}\,G^{-1}\,\sigma)\cdot\xi/4 - \mathrm{i}\sigma(\xi,\alpha)\big), \tag{5.2}$$

i.e. the covariance matrix is changed according to $\gamma \mapsto \gamma + \sigma^{\mathrm{T}}\,G^{-1}\,\sigma$, but the (average) displacement is *not* affected. This is visualized in Fig. 5.1: an initial coherent state $|\alpha\rangle\langle\alpha|$ is represented by a »lollipop stick«, where amplitude and phase are depicted by the vector α and the uncertainty is indicated by the circle corresponding to the covariance matrix $\gamma = \mathbb{1}$ (cf. Section 2.2); adding classical, uncorrelated Gaussian noise with isotropic variance g, i.e. with covariance matrix $G = \mathbb{1}/g$, enlarges the uncertainty by $\sigma^{\mathrm{T}}\,G^{-1}\,\sigma = g\,\mathbb{1}$ and hence the radius of the circle by g (the dotted and dashed circles for medium and larger g). Since the displacement is not affected, these circles are centered around the endpoint of α.

In view of the discretization we define two variants of the above channel, a cutoff version $T_{[\,]}$ where the integration is restricted to phase space translations with absolute value $|\xi| \leq a$ and its discretized counterpart T_Σ, which replaces the integration by a summation over a finite set of phase space displacements $\{\xi_k\}_{k=1,\ldots,K}$ suitable to approximate the integral:

$$T_{[\,]}(\rho) = \frac{1}{c_{[\,]}}\int\limits_{|\xi|\leq a} \mathrm{d}\xi\; \mathrm{e}^{-\xi^{\mathrm{T}}\cdot G\cdot\xi/4}\;\mathrm{W}_\xi\,\rho\,\mathrm{W}_\xi^*\,, \tag{5.3}$$

$$T_\Sigma(\rho) = \frac{1}{c_\Sigma}\sum_{k=1}^{K} \mathrm{e}^{-\xi_k^{\mathrm{T}}\cdot G\cdot\xi_k/4}\;\mathrm{W}_{\xi_k}\,\rho\,\mathrm{W}_{\xi_k}^*\,, \tag{5.4}$$

where $c_{[\,]}$ and c_Σ provide normalization. The set $\{\xi_k\}$ and the cutoff radius a remain to be determined below. For convenience, we introduce a short-hand notation for randomized coherent input states $|\alpha\rangle\langle\alpha|$ of Nf modes,

$$T(\alpha) = T\big(|\alpha\rangle\langle\alpha|\big)$$

and likewise for $T_{[\,]}(\alpha)$ and $T_\Sigma(\alpha)$. Furthermore, we can write $T(\alpha) = \mathrm{W}_\alpha\,T(0)\,\mathrm{W}_\alpha^*$ for all three flavors of T.

Repeating our task in this notation, we want to ensure that any two discretely randomized tensor products $T_\Sigma(\alpha)$ and $T_\Sigma(\beta)$ of N coherent input states with f modes each are nearly indistinguishable, $\|T_\Sigma(\alpha) - T_\Sigma(\beta)\|_1 < \epsilon$, if they obey the energy constraint $|\alpha|^2, |\beta|^2 \leq 2NfE_{\max}$, i.e. if each single mode contributes at most energy $E_{\max}$.

5.2 Security estimation

Since the relevant distinguishability $\|T_\Sigma(\alpha) - T_\Sigma(\beta)\|_1$ is not easily accessible, we use the triangle inequality and derive a bound in terms of the trace norm distances $\|T_\Sigma(\alpha) - T_{[]}(\alpha)\|_1$ and $\|T_{[]}(\alpha) - T(\alpha)\|_1$, which determine the quality of the involved approximations and can thus be bounded, and $\|T(\alpha) - T(\beta)\|_1$, which can be bounded by the relative entropy distance. These quantities are introduced by applying the triangle inequality for the trace norm:

$$\begin{aligned}\big\|T_\Sigma(\alpha) - T_\Sigma(\beta)\big\|_1 &\leq \|T_\Sigma(\alpha) - T_{[]}(\alpha)\|_1 + \|T_\Sigma(\beta) - T_{[]}(\beta)\|_1 + \|T_{[]}(\alpha) - T_{[]}(\beta)\|_1 \\ &\leq \|T_\Sigma(\alpha) - T_{[]}(\alpha)\|_1 + \|T_\Sigma(\beta) - T_{[]}(\beta)\|_1 + \|T_{[]}(\alpha) - T(\alpha)\|_1 \\ &\quad + \|T_{[]}(\beta) - T(\beta)\|_1 + \|T(\alpha) - T(\beta)\|_1 \,.\end{aligned} \tag{5.5}$$

We proceed by deriving bounds for each term. The trace norm distance of two density operators ρ, ρ' can be estimated by the relative entropy distance $S(\rho \parallel \rho') = \operatorname{tr}[\rho\,(\log\rho - \log\rho')]$ between the operators [97, Thm. 5.5]. This is used to establish

$$\big(\|T(\alpha) - T(\beta)\|_1\big)^2 \leq 2\,S\big(T(\alpha) \parallel T(\beta)\big). \tag{5.6}$$

The exponential form (2.34a) for the density operator of a Gaussian state allows to express the relative entropy in terms of the symplectic eigenvalues γ_n of its covariance matrix:

$$\begin{aligned}S\big(T(\alpha) \parallel T(\beta)\big) &= \operatorname{tr}\big[T(\alpha)\,\big(\log T(\alpha) - \log T(\beta)\big)\big] \\ &= \operatorname{tr}\big[\big(T(0) - T(\alpha-\beta)\big)\,\log T(0)\big] \quad \text{since } T(\alpha) = \mathrm{W}_\alpha\,T(0)\,\mathrm{W}_\alpha^* \\ &= \frac{1}{2}\sum_{i,j=1}^{2Nf} M'_{i,j}\,\operatorname{tr}\big[\big(T(0) - T(\alpha-\beta)\big)\,R'_i\,R'_j\big] \quad \text{by (2.35)} \\ &= \frac{1}{2}\sum_{i,j=1}^{2Nf} M'_{i,j}\Big(\operatorname{tr}\big[T(0)\,R'_i\,R'_j\big] - \operatorname{tr}\big[T(\alpha-\beta)\,R'_i\,R'_j\big]\Big) \\ &= \frac{1}{2}\sum_{i,j=1}^{2Nf} M'_{i,j}\Big(\operatorname{tr}\big[T(0)\,R'_i\,R'_j\big] - \\ &\qquad\qquad \operatorname{tr}\big[T(0)\,\big(R'_i - (\alpha'-\beta')_i\big)\,\big(R'_j - (\alpha'-\beta')_j\big)\big]\Big)\end{aligned}$$

$$= -\frac{1}{2} \sum_{i,j=1}^{2Nf} M'_{i,j} \, (\alpha' - \beta')_i \, (\alpha' - \beta')_j \,,$$

$$\text{where} \quad M' = \bigoplus_{n=1}^{Nf} \mathbb{1}_2 \, \log\left(\frac{\gamma_n - 1}{\gamma_n + 1}\right).$$

The last identity is due to the fact that $T(\alpha)$, $T(\beta)$ and $T(0)$ all possess the same covariance matrix $\gamma = \mathbb{1}_{2Nf} + \sigma^{\mathrm{T}} G^{-1} \sigma$ by (5.2) and that $T(0)$ is centered around zero, i.e. $\mathrm{tr}[T(0) R'_k] = 0$ for all field operators R'_k with $k = 1, \ldots, 2Nf$. Recall from Section 2.2.2 that the prime indicates the basis in which the covariance matrix is diagonal. For isotropic, uncorrelated Gaussian noise with $G = \mathbb{1}_{2Nf}/g$ this yields $\gamma = (1+g)\mathbb{1}_{2Nf}$ with symplectic eigenvalues $\gamma_n = 1 + g$ and thus

$$S\big(T(\alpha) \parallel T(\beta)\big) = \log(1 + 2/g) \, |\alpha - \beta|^2/2 \leq 4 \log(1 + 2/g) \, Nf E_{\max} \,.$$

Combining this estimate with (5.6) yields the bound

$$\big\|T(\alpha) - T(\beta)\big\|_1 \leq 2\sqrt{2 \log(1 + 2/g) \, Nf E_{\max}} \;, \tag{5.7}$$

which proves the functioning of the continuous randomization in the first place, since both output states can be made arbitrarily indistinguishable from each other by choosing g large enough.

As a first step towards the discrete protocol, we approximate the ideal randomization (5.1) by the cutoff integral (5.3). To estimate the error $\|T_{[\,]}(\alpha) - T(\alpha)\|_1$ we compare both channels with the nonnormalized, completely positive map $\frac{c_{[\,]}}{c} T_{[\,]}(\alpha)$:

$$\big\|T_{[\,]}(\alpha) - T(\alpha)\big\|_1 \leq \big\|T_{[\,]}(\alpha) - \tfrac{c_{[\,]}}{c} T_{[\,]}(\alpha)\big\|_1 + \big\|\tfrac{c_{[\,]}}{c} T_{[\,]}(\alpha) - T(\alpha)\big\|_1 \,. \tag{5.8}$$

Both terms will be estimated by the same bound for the difference between the full and the cutoff classical integral:

$$\begin{aligned}
\big\|T_{[\,]}(\alpha) - \tfrac{c_{[\,]}}{c} T_{[\,]}(\alpha)\big\|_1 &= \tfrac{1}{c} \, |c - c_{[\,]}| \, \big\|T_{[\,]}(\alpha)\big\|_1 \\
&= \frac{1}{c} \Big| \int \mathrm{d}\xi \; \mathrm{e}^{-\xi^{\mathrm{T}} \cdot G \cdot \xi/4} \; - \int\limits_{|\xi| \leq a} \mathrm{d}\xi \; \mathrm{e}^{-\xi^{\mathrm{T}} \cdot G \cdot \xi/4} \Big| \\
&\quad \text{since } \big\|T_{[\,]}(\alpha)\big\|_1 = 1 \\
&= \frac{1}{c} \int\limits_{|\xi| \geq a} \mathrm{d}\xi \; \mathrm{e}^{-\xi^{\mathrm{T}} \cdot G \cdot \xi/4} \,, \qquad (5.9a) \\
\big\|\tfrac{c_{[\,]}}{c} T_{[\,]}(\alpha) - T(\alpha)\big\|_1 &= \Big\| \frac{1}{c} \int\limits_{|\xi| \geq a} \mathrm{d}\xi \; \mathrm{e}^{-\xi^{\mathrm{T}} \cdot G \cdot \xi/4} \; \mathrm{W}_\xi |\alpha\rangle\langle\alpha| \, \mathrm{W}_\xi^* \Big\|_1 \\
&= \frac{1}{c} \int\limits_{|\xi| \geq a} \mathrm{d}\xi \; \mathrm{e}^{-\xi^{\mathrm{T}} \cdot G \cdot \xi/4} \qquad (5.9b) \\
&\quad \text{since } \big\|\mathrm{W}_\xi |\alpha\rangle\langle\alpha| \, \mathrm{W}_\xi^*\big\|_1 = 1.
\end{aligned}$$

This integral is estimated for isotropic, uncorrelated Gaussian noise with uniform covariance g as follows:

$$\begin{aligned}
\frac{1}{c}\int\limits_{|\xi|\geq a} \mathrm{d}\xi\, \mathrm{e}^{-\xi^{\mathrm{T}}\cdot G\cdot\xi/4} &= \left(2^{2Nf-1}\, g^{Nf}\, (Nf-1)!\right)^{-1} \int\limits_{a}^{\infty} \mathrm{d}r\; r^{2Nf-1}\, \mathrm{e}^{-r^2/(4g)} \\
&\qquad \text{by introducing polar coordinates and} \\
&\qquad \text{integrating over angular coordinates} \\
&= \left(2^{2Nf}\, g^{Nf}\, (Nf-1)!\right)^{-1} \int\limits_{a^2}^{\infty} \mathrm{d}t\; t^{Nf-1}\, \mathrm{e}^{-t/(4g)} \\
&\qquad \text{substituting } t = r^2 \\
&\leq \left(2^{2Nf}\, g^{Nf}\, (Nf-1)!\right)^{-1} \int\limits_{a^2}^{\infty} \mathrm{d}t\; \mathrm{e}^{-t/(8g)} \qquad (5.10) \\
&\qquad \text{if } a^2 \text{ is large enough to ensure that} \\
&\qquad t^{Nf-1}\, \mathrm{e}^{-t/(4g)} \leq \mathrm{e}^{-t/(8g)} \text{ for } t \geq a^2 \\
&= \left(2^{2Nf-3}\, g^{Nf-1}\, (Nf-1)!\right)^{-1} \mathrm{e}^{-a^2/(8g)}\,. \qquad (5.11)
\end{aligned}$$

Note that for the single-mode case $Nf = 1$ the inequality in the second to last line becomes an equality and there is no additional condition on a. Otherwise, the condition reads $a^2 \geq t_0$, where t_0 is the larger, real solution of $t = 8\, g\, (Nf-1) \log t$. This solution exists, if $8\, g\, (Nf-1) \geq \mathrm{e}$, which we assume to be true in the case $Nf \geq 2$ due to $g \gg 1$. Combining Eqs. (5.8), (5.9) and (5.11), we arrive at the bound

$$\left\| T_{[\,]}(\alpha) - T(\alpha) \right\|_1 \leq \left(2^{2Nf-4}\, g^{Nf-1}\, (Nf-1)!\right)^{-1} \mathrm{e}^{-a^2/(8g)}\,. \qquad (5.12)$$

In the next step, the cutoff integral (5.3) over a hypersphere of the phase space is replaced by a summation (5.4) over a discrete, regular grid of hypercubes (cf. Fig. 5.2). Each cell is labeled by a positive integer k and described by a corner point ξ_k and the characteristic function of a set, $\chi_k(\xi) = 1$ if ξ belongs to the k-th hypercube and zero otherwise. The length δ of the diagonal of the hypercubes yields the maximal distance $|\xi_k - \xi| \leq \delta$ between a point in phase space and the corner of the cell in which it is situated. The vectors ξ_k will constitute the set of encryption operations. The error introduced is estimated as follows:

$$\begin{aligned}
\left\| T_{\Sigma}(\alpha) - T_{[\,]}(\alpha) \right\|_1 = \Bigg\| \frac{1}{c_{\Sigma}} \int\limits_{|\xi|\leq a} \mathrm{d}\xi \sum_{k=1}^{K} \chi_k(\xi)\, \mathrm{e}^{-\xi_k^{\mathrm{T}}\cdot G\cdot\xi_k/4}\; \mathrm{W}_{\xi_k} |\alpha\rangle\langle\alpha|\, \mathrm{W}_{\xi_k}^{*} - \\
\frac{1}{c_{[\,]}} \int\limits_{|\xi|\leq a} \mathrm{d}\xi\; \mathrm{e}^{-\xi^{\mathrm{T}}\cdot G\cdot\xi/4}\; \mathrm{W}_{\xi} |\alpha\rangle\langle\alpha|\, \mathrm{W}_{\xi}^{*} \Bigg\|_1 ,
\end{aligned}$$

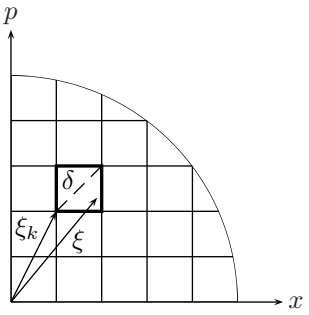


Figure 5.2:
Depicting the discretization T_Σ (5.4) of the cutoff integral in $T_{[]}$ (5.3) for a single mode (showing the upper right quadrant of phase space only). The highlighted cell is indicated by the positive integer k and described by the vector ξ_k pointing to its lower left corner. This ensures that $|\xi_k| \leq |\xi|$ for all phase space points ξ which lie in cell k, i.e. for which the characteristic function $\chi_k(\xi)$ is nonzero. The length δ of the dashed diagonal bounds the distance $|\xi_k - \xi| \leq \delta$ between ξ and the corresponding cell vector.

where the summation in the definition (5.4) of T_Σ was formally recast into an integration using the characteristic function $\chi_k(\xi)$ of the grid cells;

$$\begin{aligned}
&\leq \Big\| \frac{1}{c_\Sigma} \int\limits_{|\xi|\leq a} \mathrm{d}\xi \sum_{k=1}^{K} \chi_k(\xi) \left(\mathrm{e}^{-\xi_k^{\mathrm{T}}\cdot G\cdot \xi_k/4} - \mathrm{e}^{-\xi^{\mathrm{T}}\cdot G\cdot \xi/4} \right) \mathrm{W}_{\xi_k} |\alpha\rangle\langle\alpha| \, \mathrm{W}_{\xi_k}^* \Big\|_1 + \\
&\qquad \Big\| \left(\frac{1}{c_\Sigma} - \frac{1}{c_{[]}} \right) \int\limits_{|\xi|\leq a} \mathrm{d}\xi \, \mathrm{e}^{-\xi^{\mathrm{T}}\cdot G\cdot \xi/4} \sum_{k=1}^{K} \chi_k(\xi) \, \mathrm{W}_{\xi_k} |\alpha\rangle\langle\alpha| \, \mathrm{W}_{\xi_k}^* \Big\|_1 + \\
&\qquad \Big\| \frac{1}{c_{[]}} \int\limits_{|\xi|\leq a} \mathrm{d}\xi \, \mathrm{e}^{-\xi^{\mathrm{T}}\cdot G\cdot \xi/4} \left(\sum_{k=1}^{K} \chi_k(\xi) \, \mathrm{W}_{\xi_k} |\alpha\rangle\langle\alpha| \, \mathrm{W}_{\xi_k}^* - \mathrm{W}_\xi |\alpha\rangle\langle\alpha| \, \mathrm{W}_\xi^* \right) \Big\|_1
\end{aligned}$$

by double invocation of the triangle inequality;

$$\begin{aligned}
&\leq \frac{1}{c_\Sigma} \int\limits_{|\xi|\leq a} \mathrm{d}\xi \left| \mathrm{e}^{-\xi_k'^{\mathrm{T}}\cdot G\cdot \xi_k'/4} - \mathrm{e}^{-\xi^{\mathrm{T}}\cdot G\cdot \xi/4} \right| \left\| \mathrm{W}_{\xi_k'} |\alpha\rangle\langle\alpha| \, \mathrm{W}_{\xi_k'}^* \right\|_1 + \\
&\qquad \left| \frac{1}{c_\Sigma} - \frac{1}{c_{[]}} \right| \int\limits_{|\xi|\leq a} \mathrm{d}\xi \left| \mathrm{e}^{-\xi^{\mathrm{T}}\cdot G\cdot \xi/4} \right| \left\| \mathrm{W}_{\xi_k'} |\alpha\rangle\langle\alpha| \, \mathrm{W}_{\xi_k'}^* \right\|_1 + \\
&\qquad \frac{1}{c_{[]}} \int\limits_{|\xi|\leq a} \mathrm{d}\xi \left| \mathrm{e}^{-\xi^{\mathrm{T}}\cdot G\cdot \xi/4} \right| \left\| \mathrm{W}_{\xi_k'} |\alpha\rangle\langle\alpha| \, \mathrm{W}_{\xi_k'}^* - \mathrm{W}_\xi |\alpha\rangle\langle\alpha| \, \mathrm{W}_\xi^* \right\|_1 ,
\end{aligned} \tag{5.13}$$

where the integrations are performed piecewise over the grid cells in such a way that $\xi_k' \equiv \sum_k \chi_k(\xi)\, \xi_k$ effectively denotes the vector ξ_k of that cell to which ξ belongs.

Since $\|\mathrm{W}_{\xi'_k}|\alpha\rangle\langle\alpha|\mathrm{W}^*_{\xi'_k}\|_1 = 1$, the first term in (5.13) can be bounded in terms of the classical integral alone. We assume isotropic, uncorrelated Gaussian noise with $G = \mathbb{1}_{2Nf}/g$, perform the integration piecewise over the grid cells and bound the integrand as

$$\begin{aligned}\mathrm{e}^{-\xi_k^{\mathrm{T}}\cdot G\cdot\xi_k/4} - \mathrm{e}^{-\xi^{\mathrm{T}}\cdot G\cdot\xi/4} &= \mathrm{e}^{-\xi_k^2/(4g)} - \mathrm{e}^{-\xi^2/(4g)} \\ &= \mathrm{e}^{-\xi_k^2/(4g)}\left(1-\mathrm{e}^{-(\xi^2-\xi_k^2)/(4g)}\right) \\ &\leq \left(1-\mathrm{e}^{-|\xi^2-\xi_k^2|/(4g)}\right) \\ &\leq \left(1-\mathrm{e}^{-a\delta/(2g)}\right) \end{aligned} \tag{5.14}$$

if the integration domain is restricted to $|\xi| \leq a$ and the hypercubes constituting the grid are identified by vectors ξ_k such that $|\xi_k| \leq |\xi|$ and $|\xi - \xi_k| \leq \delta$ (see Fig. 5.2), implying that $|\xi^2 - \xi_k^2| = (\xi+\xi_k)(\xi-\xi_k) \leq 2a\delta$. Note that the scheme sketched in the caption of Fig. 5.2 requires that one of the cells is described by the vector 0; together with the cutoff radius a and the diagonal δ of the hypercubes, this already fixes the set of phase space displacements $\{\xi_k\}_{k=1,\ldots,K}$. Hence it is not necessary to communicate this set between sending and receiving parties. The integration introduces a factor of $(a^2\,\pi)^{Nf}/(Nf)!$, which is the volume of a hypersphere of radius a in dimension $2Nf$.

The second term can be reduced to the case above. Due to $\|\mathrm{W}_{\xi'_k}|\alpha\rangle\langle\alpha|\mathrm{W}^*_{\xi'_k}\|_1 = 1$ again, it suffices to consider

$$\begin{aligned}\left|\frac{1}{c_\Sigma} - \frac{1}{c_{[\,]}}\right| c_{[\,]} &= \frac{1}{c_\Sigma}\,|c_{[\,]} - c_\Sigma| \\ &\leq \frac{1}{c_\Sigma}\int\limits_{|\xi|\leq a}\mathrm{d}\xi\,\left|\mathrm{e}^{-\left(\sum_k \chi_k(\xi)\,\xi_k\right)^{\mathrm{T}}\cdot G\cdot\left(\sum_k \chi_k(\xi)\,\xi_k\right)/4} - \mathrm{e}^{-\xi^{\mathrm{T}}\cdot G\cdot\xi/4}\right| \\ &\leq \frac{1}{c_\Sigma}\,\frac{(a^2\,\pi)^{Nf}}{(Nf)!}\left(1-\mathrm{e}^{-a\delta/(2g)}\right) \end{aligned} \tag{5.15}$$

by (5.14). This is in fact the same bound as for the first term.

In order to derive a bound for the third term in (5.13), we express the trace norm distance of pure states by their fidelity [1, Ch. 9], $\left\||\psi\rangle\langle\psi| - |\phi\rangle\langle\phi|\right\|_1 = 2\sqrt{1-|\langle\psi|\phi\rangle|^2}$, and find for any given value of ξ that

$$\begin{aligned}\left\|\mathrm{W}_{\xi_k}|\alpha\rangle\langle\alpha|\,\mathrm{W}^*_{\xi_k} - \mathrm{W}_\xi|\alpha\rangle\langle\alpha|\,\mathrm{W}^*_\xi\right\|_1 &= 2\left(1-|\langle\alpha|\,\mathrm{W}^*_{\xi_k}\,\mathrm{W}_\xi\,|\alpha\rangle|^2\right)^{1/2} = \\ &2\left(1-\exp(-|\xi-\xi_k|^2/2)\right)^{1/2} \leq 2\sqrt{1-\mathrm{e}^{-\delta^2/2}}\,, \end{aligned} \tag{5.16}$$

where ξ_k identifies the hypercube in which ξ is situated and the length δ of its diagonal is the maximal distance $|\xi - \xi_k|$. This already is the bound for the third term of (5.13), since the remaining integral is normalized by $c_{[\,]}$. Combining the estimations (5.15) and (5.16) with (5.13) yields the bound

$$\begin{aligned}\left\|T_\Sigma(\alpha) - T_{[\,]}(\alpha)\right\|_1 &\leq \tfrac{2}{c_\Sigma}\,\tfrac{(a^2\,\pi)^{Nf}}{(Nf)!}\left(1-\mathrm{e}^{-a\delta/(2g)}\right) + 2\sqrt{1-\mathrm{e}^{-\delta^2/2}} \\ &\leq \tfrac{2}{c}\,\tfrac{(a^2\,\pi)^{Nf}}{(Nf)!}\left(1-\mathrm{e}^{-a\delta/(2g)}\right) + 2\sqrt{1-\mathrm{e}^{-\delta^2/2}}\,, \end{aligned} \tag{5.17}$$

where in the second line we have replaced the factor $1/c_\Sigma \leq 1/c$ for convenience.[6]

In order to guarantee the security condition $\|T_\Sigma(\alpha) - T_\Sigma(\beta)\|_1 \leq \epsilon$ we require that every term in the estimation (5.5) contributes at most $\epsilon/5$. This is accomplished through the above bounds (5.7), (5.12) and (5.17) for all coherent states $|\alpha\rangle\langle\alpha|$ and $|\beta\rangle\langle\beta|$. Additionally, we use the estimations $\log(1+x) \leq x$ and $1 - \mathrm{e}^{-x} \leq x$ for all $x \geq 0$ to obtain:

$$\left\|T(\alpha) - T(\beta)\right\|_1 \leq 4\sqrt{NfE_{\max}/g} \leq \epsilon/5\,, \tag{5.18a}$$

$$\left\|T_\Sigma(\alpha) - T_{[]}(\alpha)\right\|_1 \leq \tfrac{2}{c}\,\tfrac{(a^2\,\pi)^{Nf}}{(Nf)!}\,\tfrac{a\delta}{2g} + \sqrt{2}\,\delta \leq \epsilon/5\,, \tag{5.18b}$$

$$\left\|T_{[]}(\alpha) - T(\alpha)\right\|_1 \leq \left(2^{2Nf-4}\,g^{Nf-1}\,(Nf-1)!\right)^{-1} \mathrm{e}^{-a^2/(8g)} \leq \epsilon/5\,, \tag{5.18c}$$

subject to the additional condition from (5.10) that for $Nf \geq 2$

$$a^2 \geq t_0 \quad \text{where } t_0 \text{ is the larger, real solution of } t = 8\,g\,(Nf-1)\log t\,. \tag{5.18d}$$

From these inequalities qualitative conditions on the parameters can be readily deduced: (5.18a) is used to determine a large value for g; (5.18c) yields a large value of a in accordance with (5.18d); both terms of (5.18b) require small δ. Unfortunately, an explicit bound in the general case cannot be given for a. The first condition (5.18a) imposes

$$g \geq 400\,NfE_{\max}/\epsilon^2. \tag{5.19}$$

This bound is positive since $\epsilon, E_{\max} \geq 0$; as is to be expected, g grows with $E_{\max}$ and with shrinking security parameter ϵ. The third inequality (5.18c) formally requires

$$a \geq \sqrt{-8\,g\,\log(\epsilon\,g^{Nf-1}\,2^{2Nf-4}\,(Nf-1)!/5)}\,.$$

If the argument of the logarithm is larger than 1, then (5.18c) is true for all $a \geq 0$ and a is governed by the additional condition (5.18d). We expect this to hold true for all practical applications, except for $Nf = 1$. A bound on δ in terms of g and a can be derived from (5.18b) together with $c = (4\pi g)^{Nf}$:

$$\delta \leq \tfrac{\epsilon}{5}\left(a^{2Nf+1}\,g^{-Nf-1}\,2^{2Nf}/n! + \sqrt{2}\right)^{-1}.$$

It remains to compute the number K of hypercubes for the discretization from the volume ratio between the hypersphere with cutoff radius a and a hypercube with

6 Note that $c_\Sigma \geq c$ by the arguments leading to (5.14). With $\xi'_k \equiv \sum_k \chi_k(\xi)\,\xi_k$ as the effective ξ_k for given ξ and $G = \mathbb{1}/g$,

$$\begin{aligned} c_\Sigma - c = (c_\Sigma - c_{[]}) + (c_{[]} - c) &= \int\limits_{|\xi|\leq a} \mathrm{d}\xi\,\left(\mathrm{e}^{-\xi'^{\mathrm{T}}_k \cdot G \cdot \xi'_k/4} - \mathrm{e}^{-\xi^{\mathrm{T}}\cdot G\cdot\xi/4}\right) + \int\limits_{|\xi|\geq a} \mathrm{d}\xi\,\mathrm{e}^{-\xi^{\mathrm{T}}\cdot G\cdot\xi/4} \\ &= \int\limits_{|\xi|\leq a} \mathrm{d}\xi\,\mathrm{e}^{-\xi_k^2/(4g)}\left(1 - \mathrm{e}^{-(\xi^2-\xi_k^2)/(4g)}\right) + \int\limits_{|\xi|\geq a} \mathrm{d}\xi\,\mathrm{e}^{-\xi^2/(4g)} \geq 0 \end{aligned}$$

since both integrands are positive.

diagonal length δ (cf. Fig. 5.2). In dimension $2Nf$, the volume of the hypersphere is $V_{\mathrm{sph}} = (a^2\,\pi)^{Nf}/(Nf)!$. The hypercubes have edge length $d = \sqrt{\delta/(2Nf)}$ and thus volume $V_{\mathrm{cub}} = d^{2Nf} = \big(\delta/(2Nf)\big)^{2Nf}$. Hence the number of cells in the discretization amounts to

$$K = \frac{V_{\mathrm{sph}}}{V_{\mathrm{cub}}} = \Big(\frac{a}{\delta}\Big)^{2Nf}\ \frac{(4\pi\,N^2 f^2)^{Nf}}{(Nf)!}\,. \tag{5.20}$$

The hypercubes are labeled by the phase space vectors ξ_k, which also describe the unitary displacement operators W_{ξ_k} in the randomization. Consequently, the number of hypercubes K is the number of encryption operations. Its binary logarithm $\log_2 K$ is the number of classical bits needed to encrypt an input state under the prescribed conditions. However, our derivation is based on input states which are tensor products of N coherent states. Hence a single coherent input state is encoded by $(\log_2 K)/N$ classical bits. To decrease the number of bits per input state, a small value of a/δ is required. In principle, this could be achieved by the smallest value possible for a and the largest for δ. Unfortunately, these are interlocked with each other and g by Eq. (5.18b), which makes it problematic to determine the optimal key rate even for this specific protocol.

Single mode

In order to provide a more explicit solution, we study the special case of $Nf = 1$, i.e. single-mode input states without consideration of correlations. The conditions (5.18) together with $c = 4\pi g$ simplify to

$$\begin{aligned}
\big\|T(\alpha) - T(\beta)\big\|_1 &\leq 4\sqrt{E_{\max}/g} \leq \epsilon/5\,,\\
\big\|T_{\Sigma}(\alpha) - T_{[]}(\alpha)\big\|_1 &\leq \delta\big(a^3/(4g^2) + \sqrt{2}\big) \leq \epsilon/5\,,\\
\big\|T_{[]}(\alpha) - T(\alpha)\big\|_1 &\leq 4\,\mathrm{e}^{-a^2/(8g)} \leq \epsilon/5\,,
\end{aligned}$$

while the condition (5.18d) is irrelevant. The conditions on g, a and δ thus read:

$$\begin{aligned}
&g \geq 400\,E_{\max}/\epsilon^2,\\
&a \geq 40\,\sqrt{2E_{\max}}\,\epsilon^{-1}\,\big(\log(20/\epsilon)\big)^{1/2},\\
&\delta \leq \tfrac{\epsilon}{5}\,\big(a^3/(4g^2) + \sqrt{2}\big)^{-1}.
\end{aligned}$$

The number K of encryption operations (5.20) depends on a/δ which is bounded by

$$a/\delta \geq \tfrac{5}{\epsilon}\,\big(a^4/(4g^2) + \sqrt{2}a\big)$$

and hence computes as

$$K = 4\pi\,\Big(\frac{a}{\delta}\Big)^2 = \Big(16\,\big(\log(20/\epsilon)\big)^2 + 80\,\sqrt{E_{\max}}\,\epsilon^{-1}\,\big(\log(20/\epsilon)\big)^{1/2}\Big)^2\,.$$

5.3 Result and outlook

The calculations of the previous sections culminate in the following proposition and provide its proof:

Proposition 5.1:
A private quantum channel with approximate security and discrete classical key can be realized for coherent states by randomization with isotropic, uncorrelated Gaussian noise. The protocol can be secured against all collective attacks, including coherent schemes, involving a finite number of output states by considering tensor products of input states. In particular, any two output states $T(\alpha)$, $T(\beta)$ of the randomization T for tensor products $|\alpha\rangle\langle\alpha|$, $|\beta\rangle\langle\beta|$ of N coherent states with f modes each are nearly indistinguishable in the sense of arbitrarily small trace norm distance $\|T(\alpha) - T(\beta)\|_1 \leq \epsilon$. This is accomplished by

- ▷ addition of Gaussian noise with uniform covariance $g \geq g(\epsilon, E_{\max}, Nf)$,
- ▷ restriction to a hypersphere of radius $a \geq a(g, Nf)$ in phase space and
- ▷ discretization to $K = K(a, \delta, Nf)$ hypercubes with
- ▷ diagonal $\delta \leq \delta(a, g, Nf)$,

where the exact values are established through Eqs.(5.18) and (5.20). The encryption scheme requires $(\log_2 K)/N$ classical bits of the discrete key per input state encrypted. Moreover, the phase space displacements determining the encryption operations are defined deterministically and implicitly. Hence no preparatory communication between sending and receiving parties is needed apart from exchange of the global parameters and the classical key.

For the simplest case of single-mode coherent states without consideration of correlations, the following corollary summarizes the more explicit results derived above:

Corollary 5.2:
For $Nf = 1$ the protocol guarantees security up to ϵ, i.e. $\|T(\alpha) - T(\beta)\|_1 \leq \epsilon$, with the following parameter values:

- ▷ $g \geq 400\, E_{\max}/\epsilon^2$,
- ▷ $a \geq 40\, \sqrt{2E_{\max}}\, \epsilon^{-1} \left(\log(20/\epsilon)\right)^{1/2}$,
- ▷ $\delta \leq \frac{\epsilon}{5} \left(a^3/(4g^2) + \sqrt{2}\right)^{-1}$,
- ▷ $K = \left(16 \left(\log(20/\epsilon)\right)^2 + 80\, \sqrt{E_{\max}}\, \epsilon^{-1} \left(\log(20/\epsilon)\right)^{1/2}\right)^2$.

The above parameter values have been derived for a specific protocol and with the help of several estimations; this leaves plenty of space for optimization. A few more »technical« improvements could be achieved by finding tighter estimations for the various steps of the computation or by optimizing the contributions of the terms in (5.18). A conceptual extension could include the application of correlated

noise in the randomization, implemented by LOCC operations spanning consecutive input states. Finally, the protocol could be considerably altered by employing non-Gaussian noise, e.g. a flat distribution with finite cutoff radius, which would come nearer a randomization onto a maximally mixed state. In any case, the results of this chapter already prove that coherent states can be encrypted.

Bibliography

Bibliography

References of the form quant-ph/0509154 indicate electronic preprints from the `arXiv.org` server.

[a] N. J. Cerf, O. Krüger, P. Navez, R. F. Werner and M. M. Wolf, »Non-Gaussian Cloning of Quantum Coherent States is Optimal«, Phys. Rev. Lett. **95**, 070501 (2005).

[b] O. Krüger and R. F. Werner, »Gaussian Quantum Cellular Automata«, in *Quantum Information with continuous variables of atoms and light*, edited by N. Cerf, G. Leuchs and E. S. Polzik (Imperial College Press, London/UK, in print).

[c] D. Kretschmann and O. Krüger, »Gaussian private quantum channels for coherent states«, in preparation.

[d] O. Krüger, »Verschränktheitsmaße Gaußscher Zustände mit 1×1 Moden«, Diploma thesis (TU Braunschweig, 2001); `www.imaph.tu-bs.de/qi/papers.html`.

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge/UK, 2000).

[2] P. Shor, »Algorithms for quantum computation: discrete logarithms and factoring«, in *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, 124 (IEEE, Los Alamitos/CA, 1994).

[3] M. M. Wolf, G. Giedke and J. I. Cirac, »Extremality of Gaussian quantum states«, quant-ph/0509154 (2005).

[4] V. I. Arnold, *Mathematical Methods of Classical Mechanics*, Springer Graduate Texts in Mathematics Vol. 60 (Springer, New York, 1978).

[5] J. I. Cirac, J. Eisert, G. Giedke, M. Lewenstein, M. Plenio, R. F. Werner and M. Wolf, textbook in preparation. The preview version used is partly based on [15].

[6] A. S. Holevo, *Probabilistic and statistical aspects of quantum theory* (North-Holland, Amsterdam, 1982).

[7] M. Reed and B. Simon, *Methods of modern mathematical physics*, Vol. I and II (Academic Press, New York, 1972/1975).

[8] R. Werner, »Quantum harmonic analysis on phase space«, J. Math. Phys. **25**, 1404 (1984).

[9] E. P. Wigner, »On the Quantum Correction For Thermodynamic Equilibrium«, Phys. Rev. **40**, 749 (1932).

[10] A. Grossmann, »Parity operator and quantization of delta-functions«, Comm. Math. Phys. **48**, 191 (1976).

[11] Arvind, B. Dutta, N. Mukunda and R. Simon, »The real symplectic groups in quantum mechanics and optics«, Pramana **45**, 471 (1995); quant-ph/9509002 (1995).

[12] Arvind, B. Dutta, N. Mukunda and R. Simon, »Two-mode quantum systems: Invariant classification of squeezing transformations and squeezed states«, Phys. Rev. A **52**, 1609 (1995).

[13] R. Simon, N. Mukunda and B. Dutta, »Quantum-noise matrix for multimode systems: U(n) invariance, squeezing, and normal forms«, Phys. Rev. A **49**, 1567 (1994).

[14] R. F. Werner, »Quantum state with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model«, Phys. Rev. A **40**, 4277 (1989).

[15] M. M. Wolf, *Partial Transposition in Quantum Information Theory*, Doctoral thesis (TU Braunschweig, 2003); `www.imaph.tu-bs.de/qi/papers.html`.

[16] A. Peres, »Separability Criterion for Density Matrices«, Phys. Rev. Lett. **77**, 1413 (1996).

[17] M. Horodecki, P. Horodecki and R. Horodecki, »Separability of mixed states: necessary and sufficient conditions«, Phys. Lett. A **223**, 1 (1996).

[18] R. F. Werner and M. M. Wolf, »Bound Entangled Gaussian States«, Phys. Rev. Lett. **86**, 3658 (2001).

[19] M. Takesaki, *Theory of Operator Algebras*, Vol. I (Springer, New York, 1979).

[20] B. Demoen, P. Vanheuverzwijn and A. Verbeure, »Completely positive maps on the CCR-algebra«, Lett. Math. Phys. **2**, 161 (1977).

[21] B. Demoen, P. Vanheuverzwijn and A. Verbeure, »Completely positive quasi-free maps of the CCR-algebra«, Rep. Math. Phys. **15**, 27 (1979).

[22] A. S. Holevo and R. F. Werner, »Evaluating capacities of bosonic Gaussian channels«, Phys. Rev. A **63**, 032312 (2001).

[23] J. Eisert and M. B. Plenio, »Conditions for the Local Manipulation of Gaussian States«, Phys. Rev. Lett. **89**, 097901 (2002).

[24] J. Fiurášek, »Gaussian Transformations and Distillation of Entangled Gaussian States«, Phys. Rev. Lett. **89**, 137904 (2002).

[25] K. Kraus, *States, Effects and Operations*, edited by A. Bohm, J. D. Dollard and W. H. Wootters (Springer, Berlin, 1983).

[26] W. K. Wooters and W. H. Zurek, »A single quantum cannot be cloned«, Nature (London) **299**, 802 (1982).

[27] H. Barnum, C. M. Caves, C. A. Fuchs, R. Josza and B. Schumacher, »Noncommuting Mixed States Cannot Be Broadcast«, Phys. Rev. Lett. **76**, 2818 (1996).

[28] R. F. Werner, »Quantum information theory – an invitation«, in *Quantum Information – An Introduction to Basic Theoretical Concepts and Experiments*, by G. Alber et al., Springer Tracts in Modern Physics Vol. 173 (Springer, Berlin, 2001).

[29] R. F. Werner, »The Uncertainty Relation for Joint Measurement of Position and Momentum«, in *Quantum Information, Statistics, Probability*, edited by O. Hirota (Rinton, Princeton/NJ, 2004).

[30] F. Grosshans and N. J. Cerf, »Continuous-Variable Quantum Cryptography is Secure against Non-Gaussian Attacks«, Phys. Rev. Lett. **92**, 047905 (2004).

[31] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf and P. Grangier, »Quantum key distribution using gaussian-modulated coherent states«, Nature (London) **421**, 238 (2003).

[32] S. Iblisdir, G. Van Assche and N. J. Cerf, »Security of Quantum Key Distribution with Coherent States and Homodyne Detection«, Phys. Rev. Lett. **93**, 170502 (2004).

[33] V. Bužek and M. Hillery, »Quantum copying: Beyond the no-cloning theorem«, Phys. Rev. A **54**, 1844 (1996).

[34] N. Gisin and S. Massar, »Optimal Quantum Cloning Machines«, Phys. Rev. Lett. **79**, 2153 (1997).

[35] D. Bruss, D. P. DiVincenzo, A. Ekert, C. A. Fuchs, C. Macchiavello and J. A. Smolin, »Optimal universal and state-dependent quantum cloning«, Phys. Rev. A **57**, 2368 (1998).

[36] V. Bužek and M. Hillery, »Universal optimal cloning of qubits and quantum registers«, in *Proceedings of the 1st* NASA *Int. Conf. on Quantum Computing and Communications* (1998) and quant-ph/9801009 (1998); »Universal optimal cloning of arbitrary quantum states: from qubits to quantum registers«, Phys. Rev. Lett **81**, 5003 (1998).

[37] R. F. Werner, »Optimal cloning of pure states«, Phys. Rev. A **58**, 1827 (1998).

[38] J. Fiurášek, R. Filip and N. J. Cerf, »Highly asymmetric quantum cloning in arbitrary dimension«, quant-ph/0505212 (2005).

[39] M. Keyl and R. F. Werner, »Optimal cloning of pure states, testing single clones«, J. Math. Phys. **40**, 3283 (1999).

[40] C. A. Fuchs and C. M. Caves, »Mathematical Techniques for Quantum Communication Theory«, Open Sys. Inf. Dyn. **3**, 345 (1995).

[41] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa and B. Schumacher, »Noncommuting mixed states cannot be broadcast«, Phys. Rev. Lett. **76**, 2818 (1996).

[42] E. Hewitt and K. A. Ross, *Abstract harmonic analysis*, Vol. I, Chapter IV.§17 (Springer, Berlin, 1963).

[43] R. F. Werner, unpublished.

[44] M. Keyl, D. Schlingemann and R. F. Werner, »Infinitely entangled states«, Quant. Inf. Comp. **3**, 281 (2003).

[45] M. M. Wolf, unpublished.

[46] K. Hammerer, M. M. Wolf, E. S. Polzik and J. I. Cirac, »Quantum Benchmark for Storage and Transmission of Coherent States«, Phys. Rev. Lett. **94**, 150503 (2005).

[47] N. Cerf, »Quantum cloning with continuous variables«, in *Quantum Information with Continuous Variables*, edited by S. L. Braunstein and A. K. Pati (Kluwer, Dordrecht, 2003).

[48] N. J. Cerf and S. Iblisdir, »Universal copying of coherent states: a Gaussian cloning machine«, in *Quantum Communication, Computing, and Measurement 3*, edited by P. Tombesi and O. Hirota (Kluwer, Dordrecht, 2001).

[49] S. L. Braunstein, N. J. Cerf, S. Iblisdir, P. van Loock and S. Massar, »Optimal Cloning of Coherent States with a Linear Amplifier and Beam Splitters«, Phys. Rev. Lett. **86**, 4938 (2001).

[50] J. Fiurášek, »Optical Implementation of Continuous-Variable Quantum Cloning Machines«, Phys. Rev. Lett. **86**, 4942 (2001).

[51] J. Fiurášek, »Optimal probabilistic cloning and purification of quantum states«, Phys. Rev. A **70**, 032308 (2004).

[52] C. M. Caves, »Quantum limits on noise in linear amplifiers«, Phys. Rev. D. **26**, 1817 (1982).

[53] G. Lindblad, »Cloning the quantum oscillator«, J. Phys. A **33**, 5059 (2000).

[54] N. J. Cerf, A. Ipe and X. Rottenberg, »Cloning of Continuous Quantum Variables«, Phys. Rev. Lett. **85**, 1754 (2000).

[55] N. J. Cerf and S. Iblisdir, »Optimal N-to-M cloning of conjugate quantum variables«, Phys. Rev. A **62**, 040301 (2000).

[56] U. L. Andersen, V. Josse and G. Leuchs, »Unconditional Quantum Cloning of Coherent States with Linear Optics«, Phys. Rev. Lett. **94**, 240503 (2005).

[57] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres and W. K. Wootters, »Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels«, Phys. Rev. Lett. **70**, 1895 (1993).

[58] L. Vaidman, »Teleportation of quantum states«, Phys. Rev. A **49**, 1473 (1994).

[59] S. L. Braunstein and H. J. Kimble, »Teleportation of Continuous Quantum Variables«, Phys. Rev. Lett. **80**, 869 (1998).

[60] C. M. Caves and K. Wódkiewicz, »Classical Phase-Space Descriptions of Continuous-Variable Teleportation«, Phys. Rev. Lett. **93**, 040506 (2004).

[61] C. M. Caves and K. Wódkiewicz, »Fidelity of Gaussian channels«, Open Sys. Inf. Dynamics **11**, 309 (2004).

[62] G. Adesso and F. Illuminati, »Equivalence between Entanglement and the Optimal Fidelity of Continuous Variable Teleportation«, Phys. Rev. Lett. **95**, 150503 (2005).

[63] S. L. Braunstein, C. A. Fuchs and H. J. Kimble, »Criteria for continuous-variable quantum teleportation«, J. Mod. Opt. **47**, 267 (2000).

[64] S. L. Braunstein, C. A. Fuchs, H. J. Kimble and P. van Loock, »Quantum versus classical domains for teleportation with continuous variables«, Phys. Rev. A **64**, 022321 (2001).

[65] F. Grosshans and P. Grangier, »Quantum cloning and teleportation criteria for continuous quantum variables«, Phys. Rev. A **64**, 010301 (2001).

[66] A. Furusawa, J. L. Sørensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble and E. S. Polzik, »Unconditional quantum teleportation«, Science **282**, 706 (1998).

[67] W. P. Bowen, N. Treps, B. C. Buchler, R. Schnabel, T. C. Ralph, H. A. Bachor, T. Symul and P. K. Lam, »Experimental investigation of continuous-variable quantum teleportation«, Phys. Rev. A **67**, 032302 (2003).

[68] T. C. Zhang, K. W. Goh, C. W. Chou, P. Lodahl and H. J. Kimble, »Quantum teleportation of light beams«, Phys. Rev. A **67**, 033802 (2003).

[69] N. Takei, H. Yonezawa, T. Aoki and A. Furusawa, »High-Fidelity Teleportation beyond the No-Cloning Limit and Entanglement Swapping for Continuous Variables«, Phys. Rev. Lett. **94**, 220502 (2005).

[70] B. Schumacher and R. F. Werner, »Reversible quantum cellular automata«, quant-ph/0405174 (2004).

[71] B. Chopard and M. Droz, *Cellular Automata Modeling of Physical Systems* (Cambridge University Press, Cambridge/UK, 1998).

[72] E. R. Berlekamp, J. H. Conway and R. K. Guy, *Winning Ways for your mathematical plays* (Academic Press, London/UK, 1982).

[73] R. Feynman, »Simulating physics with computers«, Int. J. Theor. Phys. **21**, 467 (1982); reprinted in *Feynman and Computation – Exploring the Limits of Computers*, edited by A. J. G. Hey (Perseus, Reading/MA, 1999).

[74] J. Watrous, »On one-dimensional quantum cellular automata«, in *Proceedings of* IEEE *36th Annual Foundations of Computer Science*, 528 (IEEE Press, Los Alamitos/CA, 1995).

[75] W. van Dam, »A Universal Quantum Cellular Automaton«, in *Proceedings of PhysComp96*, edited by T. Toffoli, M. Biafore and J. Leão, 323 (New England Complex Systems Institute, Boston/MA, 1996); InterJournal manuscript 91 (1996).

[76] R. Raussendorf, »A quantum cellular automaton for universal quantum computation«, Phys. Rev. A **72**, 022301 (2005).

[77] R. Raussendorf, »Quantum computation via translation-invariant operations on a chain of qubits«, Phys. Rev. A **72**, 052301 (2005).

[78] D. J. Shepherd, T. Franz and R. F. Werner, »A universally programmable Quantum Cellular Automaton«, quant-ph/0512058 (2005).

[79] K. G. H. Vollbrecht, E. Solano and J. I. Cirac, »Ensemble quantum computation with atoms in periodic potentials«, Phys. Rev. Lett. **93**, 220502 (2004).

[80] K. G. H. Vollbrecht and J. I. Cirac, »Reversible universal quantum computation within translation invariant systems«, quant-ph/0502143 (2005).

[81] O. Mandel, M. Greiner, A. Widera, T. Rom, T. W. Hänsch and I. Bloch, »Coherent Transport of Neutral Atoms in Spin-Dependent Optical Lattice Potentials«, Phys. Rev. Lett. **91**, 010407 (2003).

[82] R. Dumke, M. Volk, T. Mühter, F. B. J. Buchkremer, G. Birkel and W. Ertmer, »Microoptical Realization of Arrays of Selectively Addressable Dipole Traps: A Scalable Configuration for Quantum Computation with Atomic Qubits«, Phys. Rev. Lett. **89**, 097903 (2002).

[83] J. Kempe, »Quantum random walks: an introductory overview«, Contemp. Phys. **44**, 307 (2003).

[84] O. Bratelli and D. W. Robinson, *Operator algebras and quantum statistical mechanics* (Springer, New York, 1979).

[85] C. D. Cushen and R. L. Hudson, »A quantum-mechanical central limit theorem«, J. Appl. Prob. **8**, 454 (1971).

[86] E. B. Davies, »Quantum Stochastic Processes«, Comm. Math. Phys. **15**, 277 (1969).

[87] E. B. Davies, »Diffusion for Weakly Coupled Quantum Oscillators«, Comm. Math. Phys. **27**, 309 (1972).

[88] S. Richter and R. F. Werner, »Ergodicity of quantum cellular automata«, J. Stat. Phys. **82**, 963 (1996).

[89] T. Eggeling, D. Schlingemann and R. F. Werner, »Semicausal operations are semilocalizable«, Europhys. Lett. **57**, 782 (2002).

[90] P. O. Boykin and V. Roychowdhury, »Optimal Encryption of Quantum Bits«, Phys. Rev. A **67**, 042317 (2003).

[91] A. Ambainis, M. Mosca, A. Tapp and R. de Wolf, »Private Quantum Channels«, in *Proceedings of the 41st Annual Symposium on Foundations of Computer Science*, 547 (IEEE, Los Alamitos/CA, 2000).

[92] M. Mosca, A. Tapp and R. de Wolf, »Private Quantum Channels and the Cost of Randomizing Quantum Information«, quant-ph/0003101 (2000).

[93] H. Azuma and M. Ban, »A method of enciphering quantum states«, J. Phys. A **34**, 2723 (2001).

[94] P. Hayden, D. Leung, P. W. Shor and A. Winter, »Randomizing quantum states: Constructions and applications«, Comm. Math. Phys. **250**, 371 (2004).

[95] A. Ambainis and A. Smith, »Small Pseudo-Random Families of Matrices: Derandomizing Approximate Quantum Encryption«, in *Proceedings of the 7th International Workshop on Approximation Algorithms for Combinatorial Optimization Problems* APPROX 2004 *and the 8th International Workshop on Radomization and Computation* RANDOM 2004, 249 (Springer, Heidelberg, 2004).

[96] K. Brádler, »Continuous variable private quantum channel«, quant-ph/0505118 (2005).

[97] M. Ohya and D. Petz, *Quantum entropy and its use* (Springer, Berlin, 1993).

Dank

An erster Stelle bedanke ich mich bei Prof. Reinhard Werner für die kompetente und engagierte Betreuung dieser Arbeit und für die vielfältigen Einblicke in die Mathematische Physik.

Außerdem möchte ich danken

Michael Wolf für die spannende Zusammenarbeit und wesentliche Verbesserungsvorschläge bei der Entstehung dieser Arbeit.

Dennis Kretschmann für die angenehme Nachbarschaft und die Zusammenarbeit über die Grenzen kohärenter Zustände hinweg.

Fabian Heidrich-Meisner für die gemeinsame Studienzeit in Braunschweig.

Dirk Schlingemann für seine Antworten auf meine Fragen und die vielfältigen Beiträge zu den Mittagsdiskussionen.

Michael Reimpell für das Fachsimpeln.

Conny Schmidt für ihre gute Laune und den Überblick.

Den Korrekturlesern dieser Arbeit für ihre Zeit und die hilfreichen Kommentare: Conny, Dennis, Fabian, Michael und Torsten.

Allen Mitgliedern der AG Quanteninformation für die schöne Zeit und die unzähligen anregenden Gespräche beim Mittagskaffee.

Weiterhin bin ich der Studienstiftung des deutschen Volkes zu großem Dank für meine Förderung verpflichtet.

Schließlich danke ich ganz besonders Caroline und meinen Eltern für ihr Verständnis, ihre Unterstützung und die Geduld, mit der sie das Entstehen dieser Dissertation durchgestanden haben.

Vielen Dank!

Braunschweig, Dezember 2005
Ole Krüger