UNIVERSITY OF LONDON

Imperial College London
Institute for Mathematical Sciences

Computational power of quantum many-body states and some results on discrete phase spaces

David Gross

Thesis submitted in partial fulfilment of the requirements for
the degree of Doctor of Philosophy of the University of London
and the Diploma of Membership of Imperial College.

JULY 2008

Abstract

This thesis consists of two parts.

The main part is concerned with new schemes for measurement-based quantum computation. Computers utilizing the laws of quantum mechanics promise an exponential speed-up over purely classical devices. Recently, considerable attention has been paid to the measurement-based paradigm of quantum computers. It has been realized that local measurements on certain highly entangled quantum states are computationally as powerful as the well-established model for quantum computation based on controlled unitary evolution.

Prior to this thesis, only one family of quantum states was known to possess this computational power: the so-called cluster state and some very close relatives. Questions posed and answered in this thesis include: Can one find families of states different from the cluster, which constitute universal resources for measurement-based computation? Can the highly singular properties of the cluster state be relaxed while retaining universality? Is the quality of being a computational resource common or rare among pure states?

We start by establishing a new mathematical tool for understanding the connection between local measurements on an entangled quantum state and a quantum computation. This framework – based on finitely correlated states (or matrix product states) common in many-body physics – is the first such tool general enough to apply to a wide range of quantum states beyond the family of graph states. We employ it to construct a variety of new universal resource states and schemes for measurement-based computation. It is found that many entanglement properties of universal states may be radically different from those of the cluster: we identify states which are locally arbitrarily close to a pure state, exhibit long-ranged correlations or cannot be converted into cluster states by means of stochastic local operations and

classical communication. Flexible schemes for the compensation of the inherent randomness of quantum measurements are introduced. We proceed to provide a complete classification of a natural class of states which can take the role of a single logical qubit in a measurement-based quantum computer. Lastly, it is demonstrated that states can be too entangled to be useful for any computational purpose. Concentration of measure arguments show that this problem occurs for the dramatic majority of all pure states.

The second part of the thesis is concerned with discrete quantum phase spaces. We prove that the only pure states to possess a non-negative Wigner function are stabilizer states. The result can be seen as a finite-dimensional analogue of a classic theorem due to Hudson, who showed that Gaussian states play the same role in the setting of continuous variable systems. The quantum phase space techniques developed for this argument are subsequently used to quantize a well-known structure from classical computer science: the Margulis expander.

To my wife

This thesis was written under the supervision of J. Eisert.

Contents

List of Figures

Part I

Computational power of quantum many-body states

In the standard model of quantum computation, a set of two-level systems initially in a product state is subjected to a unitary time-evolution in the form of sequential bipartite quantum gates [82]. At the end of the evolution, the systems are measured in some local basis, in order to read out the result of the computation. Such gate-model quantum computers are strongly believed to offer a super-polynomial speed-up over classical machines. One may attribute this computational power to the intractability of simulating the time evolution in an exponentially large Hilbert space.

From that point of view, it seems surprising that universal quantum computation is possible without the need of unitary evolution at all. But indeed, the *one-way model* of Refs. [89, 90] demonstrates that local measurements on the *cluster state* – a certain multi-particle entangled state on an array of qubits [16] – are computationally as powerful as any gate-model computation. The local measurements – a feature that any computing scheme would eventually embody – then take the role of preparation of the input, the computation proper, and the read-out. In such a setting, quantum computation merely amounts to (i) preparing an algorithm-independent resource state and (ii) performing local projective measurements [16, 18, 54, 64, 81, 89, 90].

Faced with this result, some obvious questions suggest themselves. First, concentrating on the *quantum states* which provide the computational power of measurement-based schemes, one may ask

1. *What are the properties that render a state a universal resource for a measurement-based computing scheme?*

Secondly, putting the emphasize on *methods*, the central question becomes

2. *How can we systematically construct new schemes for measurement-based quantum computation? Is there a framework which is flexible enough to allow for the construction of a variety of different models?*

Such questions are clearly relevant from a practical point of view. What if the states that naturally occur in some physical situation are different from cluster states or graph states [54, 55, 97]? Is it possible to tailor resource states to specific physical systems? For some experimental implementations – e.g., cold atoms in optical lattices [75], atoms

in cavities [19, 21, 23, 49], optical systems [11], [20, 120], ions in traps [47], or many-body ground states – it may well be that preparation of cluster states is unfeasible, costly, or that they are particularly fragile to finite temperature or decoherence effects.

Adopting a more fundamental position, it is clearly interesting to investigate the computational power of many-body states – either for the purpose of building measurement-based quantum computers, or else for deciding which states could possibly be classically simulated [63, 100, 108].

Interestingly, very little progress has been made over the last years when it comes to going beyond the cluster state as a resource for measurement-based quantum computation (MBQC). To the knowledge of the author, no single computational model distinct from the one-way computer has been developed which would be based on local measurements on an algorithm-independent qubit resource state.

Our contributions to understanding the computational power of quantum many-body states are organized in three chapters.

Chapter 1 establishes the existence of a diverse set of universal resource states beyond the cluster. Methods for the systematic construction of new MBQC schemes and states are described. We introduce the notion of "computational tensor networks", building on a familiar tool from many-body physics known by the names of finitely correlated states [35], matrix product states [83, 84] or projected entangled pair states [2, 112]. Using these methods, we go on to show that entanglement properties of universal states may be radically different from those of the cluster.

Chapter 2 – Having shown that the cluster is not unique in constituting a universal resource, it is natural to ask whether a complete classification of resource states is possible. The unqualified version of this question seems daunting. Fortunately, it turns out that a complete classification becomes tractable once certain natural extra assumptions about resource states are made. This is the content of Chapter 2. More specifically, we initiate the study of *computational quantum wires* – states on one-dimensional chains of quantum systems, which may be interpreted as the measurement-based equivalent of a single qubit. All qubit wires which can be prepared by sequentially entangling neighboring systems are classified and many of their properties are explicitly calculated. We show how to couple such one-dimensional wires together to obtain a computationally

universal resource state.

Chapter 3 – Even though Chapters 1 and 2 present a plethora of new universal resource, it is still fair to say that "most" states elude our methods. Tailoring a computational scheme to a given state is a painstaking process which relies on a host of coincidental properties: by-product groups must close, logical evolution must be unitary, it must be possible to de-couple logical qubits and so on (these notions will be made precise in Chapter 1). An obvious question to ask is whether these problems are owed to a yet incomplete understanding of measurement-based computation, or whether "universality" is truly a rare property among quantum states. In this chapter we show that the latter scenario is realized: almost all states are too entangled to be useful.

All results presented in this part are joint work with J. Eisert. Parts of Chapter 1 result from a collaboration with N. Schuch and D. Perez-Garcia. The statements in Chapter 3 were derived by the author as part of a joint project with S. Flammia.

1

New schemes for measurement-based computation based on computational tensor networks

1.1 Introduction

1.1.1 Main results

As our main result, we present a plethora of new universal resource states and computational schemes for MBQC. The examples have been chosen to demonstrate the flexibility one has when constructing models for measurement-based computation. Indeed, it turns out that many properties one might naturally conjecture to be necessary for a state to be a universal resource can in fact be relaxed. Needless to say, the weaker the requirements are for a many-body state to form a resource for quantum computing, the more feasible physical implementations of MBQC become.

Below, we enumerate some specific results concerning the properties of resource states. The list pertains to Question 1 given in the introduction.

- In the cluster state, every particle is maximally entangled with the rest of the lattice. Also, the localizable entanglement [88] is maximal (i.e. one can deterministically prepare an maximally entangled state between any two sites, by performing local measurements on the remainder). While both properties are essential for the original one-way computer, they turn out not to be necessary for computationally universal resource states. To the contrary, we construct *universal states which are locally arbitrarily pure*.

- For previously known schemes for MBQC, it was essential that far-apart regions of the state were uncorrelated. This feature allowed one to logically break down a measurement-based calculation into small parts corresponding to individual quantum gates. Our framework does not depend on this restriction and resources with *non-vanishing correlations* between any two subsystems are shown to exist. This property is common e.g., in many-body ground-states.

- Cluster states can be prepared step-wise by means of a bi-partite *entangling gate* (controlled-phase gate). This property has been used in the original universality proof. More generally, one might conjecture that resource states must always result from an entangling process making use of mutually commuting entangling

gates, also known as a unitary *quantum cellular automaton* [99]. Once more, this requirement turns out not to be necessary.

- The cluster states can be used as *universal preparators*: Any quantum state can be distilled out of a sufficiently large cluster state by local measurements. Once more, this property is essential to the original one-way computer scheme. However, computationally universal resource states not exhibiting this properties do exist (the reader is referred to Ref. [109] for an analysis of resource states which are required to be preparators; see also the discussion in Section 1.1.3). More strongly, we construct universal resources out of which not even a single two-qubit maximally entangled state can be distilled.

- A genuine *qu-trit* resource is presented (distinct, of course, from a qu-trit version of the cluster state [127]).

We will further see that there is quite some flexibility concerning the computational model itself (addressing Question 2 mentioned in the introduction):

- The new schemes differ from the one-way model in the way the *inherent randomness* of quantum measurements is dealt with.

- We generalize the well-known concept of *by-product operators* to encompass any finite group. E.g. we show the existence of computational models, where the by-product operators are elements of the entire single-qubit Clifford group, or the dihedral group.

- We explore schemes where each logical qubit is encoded in *several neighboring correlation systems* (see Section 1.2 for a definition of the term “correlation system”).

- One can find ways to construct schemes in which interactions between logical qubits are controlled by “routing” the qubits towards an “interaction zone” or keeping them away from it.

- In many schemes, we adjust the layout of the measurement pattern dynamically, incorporating information about previous measurement outcomes as we go along.

In particular, the expected length of a computation is random (this constitutes no problem, as the probability of exceeding a finite expected length is exponentially small in the excess).

1.1.2 Previous work

The apparent lack of new schemes for MBQC is all the more surprising, given the great advances that have been made toward understanding the structure of cluster state-based computing itself. For example, it has been shown that the computational model of the one-way computer and teleportation-based approaches to quantum computing [41] are essentially equivalent [4, 62, 64]. A particularly elegant way of realizing this equivalence was discovered in Ref. [113]: They pointed out that the maximally entangled states used for the teleportation need not be physical. Instead, the role can be taken on by virtual entangled pairs used in a "valence bond" [2] description of the cluster state. This point of view is closely related to our approach to be described in Chapter 1. Further progress includes a clarification of the temporal inter-dependence of measurements [29]. In Ref. [105] a first non-cluster (though not universal, but algorithm-dependent) resource has been introduced, which includes the natural ability of performing three-qubit gates. Recently, Refs. [107, 109] initiated a detailed study of resource states which can be used to prepare cluster states. A more fine-grained study of the computational power of resource states can be found in Ref. [6], where it is shown that local measurements on a resource state can allow a limited classical computer to attain *classical* universality.

After the contents of this chapter were first published [6, 8], other authors utilized the techniques developed here to tailor models to specific physical setups [110], or to construct computational schemes with intrinsic resilience against noise [15].

1.1.3 Universal resource states

What are the properties from which a universal resource state derives its power? After clarifying the terminology, we will argue that an answer to this question – desirable as it may be – faces formidable obstacles.

Quantum computation can come in a variety of different incarnations, as diverse as e.g., the well-known gate-model [82], adiabatic quantum computation [3] or MBQC. All

these models turn out to be equivalent in that they can simulate each other efficiently.

For measurement-based schemes, the "hardware" consists of a multi-particle quantum system in an algorithm-independent state and a classical computer. The input is a gate-model description of a quantum computation. In every step of the computation, a local measurement is performed on the quantum state and the result is fed into the classical computer. Based on the outcomes of previous steps, the computer calculates which basis to use for the next measurements and, finally, infers the result of the computation from the measurement outcomes [90]. Having this procedure in mind, we call a quantum state a *universal resource* for MBQC, if a classical computer assisted by local measurements on this states can efficiently predict the outcome of any quantum computation.

The reader should be aware that another approach has recently been described in the literature. The cluster state has actually a stronger property than the one just used for the definition of universality: it is a universal preparator. This means that one can prepare any given quantum state on a given sub-set of sites of a sufficiently large cluster by means of local measurements. Hence, cluster states could in principle be used for information processing tasks which require a quantum output. Ref. [107] referred to this scenario as *CQ-universality* – i.e. universality for problems which require a classical input but deliver a quantum output. This observation is the basis of Ref. [109], where a state is called a universal resource if it possesses the strong property of being a universal preparator, or, equivalently, of being CQ-universal.

Clearly, any efficient universal preparator is also a computationally universal resource for MBQC (since one can, in particular, prepare the cluster state). But the converse is not true, as our results show. Indeed, while it proves possible to come up with necessary criteria for a state to be a universal preparator [109], we will argue below that the current limited understanding of quantum computers makes it extremely hard to specify necessary conditions for computational universality.

In order to pinpoint the source of the quantum speedup, we might try to find schemes where more and more work is done by the classical computer, while the employed quantum states become "simpler" (e.g., smaller or less entangled). How far can we push this program without losing universality? The answer is likely to be intractable. Currently,

we are not aware of a proof that quantum computation is indeed more powerful than classical methods. Hence, it can presently not be excluded that no assistance from a quantum state is necessary at all.

Observation 1 (Any state may be a universal resource)**.** *If one is unwilling to* assume *that there is a separation between classical and quantum computation (i.e., BPP $\neq$ BQP), then it is impossible to rule out any state as a universal resource.*

It is, however, both common and sensible to assume superiority of quantum computers and we will from now on do so. Observation 1 still serves a purpose: it teaches us that the only known way to rule out universality is to invoke this assumption (this avenue was taken, e.g., in Refs. [14, 108]).

Observation 2 (Efficient classical simulation)**.** *The only currently known method for excluding the possibility that a given quantum state forms a universal resource is to show that any measurement-based scheme utilizing the state can be efficiently simulated by a classical computer.*

In a previous publication [8], this observation was followed by the paragraph:

> Thus, the situation presents itself as follows: there is a tiny set of quantum states for which it is possible to prove that any local measurement-based scheme can be efficiently simulated. On the other extreme, there is an even tinier set for which universality is provable. For the vast majority no assessment can be made. Furthermore, given the fact that rigorously establishing the "hardness" of many important problems in computer science turned out to be extremely challenging, it seems unlikely that this situation will change dramatically in the foreseeable future.

This assessment proved to be too pessimistic, as shown in Chapter 3.

Still, we conclude that a search for an explicit necessary condition for universality is likely to remain futile. The converse question, however, can be pursued: it is possible to show that many properties that one might naively assume to be present in any universal resource are, in fact, unnecessary.

1.2 Computational tensor networks

The current section is devoted to an in-depth treatment of a class of states known respectively as valence-bond states, finitely correlated states, matrix product states or projected entangled pairs states, adapted to our purposes of measurement-based quantum computing. This family turns out to be especially well-suited for a description of a computing scheme.

Indeed, any systematic analysis of resources states requires a framework for describing quantum states on extended systems. We briefly compile a list of desiderata, based on which candidate techniques can be assessed.

- The description should be *scalable*, so that a class of states on systems of arbitrary size can be treated efficiently.
- As quantum states which are naturally described in terms of one-dimensional topologies have been shown to be classically simulable [35, 63, 100, 108, 115], the framework ought to handle *two- or higher dimensional topologies* naturally.
- The basic operation in measurement-based computation are *local measurements*. It would be desirable to describe the effect of local measurements in a local manner. Ideally, the class of efficiently describable states should be closed under local measurements.
- The class of describable states should include elements which show features that naturally occur in *ground states* of quantum many-body systems, such as *non-maximal local entropy of entanglement* or *non-vanishing two-point correlations*, etc.

The description of states to be introduced below complies with all of these points.

We will introduce the construction in several steps, starting with one-dimensional matrix product states. The new view on the processing of information is that the matrices appearing in the description of resource states are taken literally, as operators processing quantum information.

1.2.1 Matrix product states

A *matrix product state* (MPS) for a chain of n systems of physical dimension d (so $d = 2$ for qubits) is specified by

- An *auxiliary D dimensional vector space* (D being some parameter, describing the amount of correlation between two consecutive blocks of the chain),
- For each system i a set of d $D \times D$*-matrices* $A_i[j], j \in \{0 \dots d-1\}$.
- Two D-dimensional vectors $|L\rangle, |R\rangle$ representing *boundary conditions*.

The state vector $|\Psi\rangle$ of the matrix product state is then given explicitly by [1]

$$|\Psi\rangle = \sum_{s_1,\dots,s_n=0}^{d-1} \langle R|A_n[s_n] \dots A_1[s_1]|L\rangle \; |s_1, \dots, s_n\rangle. \tag{1.2}$$

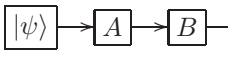
From now on we will assume that the matrices are site-independent: $A_i[j] = A[j]$, so the MPS is translationally invariant up to the boundary conditions. We take the freedom of disregarding normalization whenever this consistently possible.

Let us spend a minute interpreting Eq. (1.2). Assume we have measured the first site in the computational basis and obtained the outcome s_1. One immediately sees that the resulting state vector $|\Psi'(s_1)\rangle$ on the remaining sites is again a MPS, where the left-hand side boundary vector now reads

$$|L'(s_1)\rangle = A[s_1]|L\rangle. \tag{1.3}$$

Hence the state of the auxiliary system gets changed according to the measurement outcome. So we find that the correlations between the state of the first site and the rest of the chain are mediated via the auxiliary space, which will thus be referred to as *correlation space* in the sequel.

[1] There is a reason why the *right*-hand-side boundary condition $|R\rangle$ appears on the *left* of Eq. (1.2). In linear algebra formulas, information usually flows from right to left: $BA|\psi\rangle$ means "$|\psi\rangle$ is acted on by A, then by B". In the graphical notation to be introduce later, it is much more natural to let information flow from left to right:



(1.1)

The order in Eq. (1.2) anticipates the graphical notation.

In the past, the matrices appearing in the definition of $|\Psi\rangle$ have been treated mainly as a collection of variational parameters, used to parametrize ansatz states for ground states of spin chains [35, 83, 98]. However – and that is the basic insight underlying our view on MBQC – Eq. (1.3) can also be read as an operator $A[s_1]$ acting on some quantum state $|L\rangle$. We will elaborate on this interpretation in Section 1.2.2.

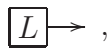
In order to translate Eq. (1.2) to the setting of 2-D lattices, we need to cast it into the form of a tensor network. Setting $L_i = \langle i|L\rangle$ and

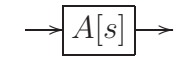
$$A[s]_{i,j} := \langle j|A|i\rangle, \tag{1.4}$$

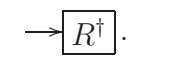
we can write Eq. (1.2) as

$$\langle s_1, \ldots, s_n|\Psi\rangle = \sum_{i_0,\ldots,i_n}^{D} L_{i_0} A[s_1]_{i_0,i_1} \ldots A[s_n]_{i_{n-1},i_n} R^\dagger{}_{i_n}. \tag{1.5}$$

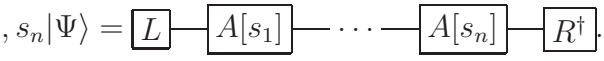
While Eq. (1.5) is awkward enough, the 2-D equivalent is completely unintelligible. To cure this problem, we introduce a graphical notation[2] which enables an intuitive understanding beyond the 1-D case. In the following, tensors will be represented by boxes, indices by edges:

L_r =  , (1.6)

$A[s]_{l,r}$ =  , (1.7)

$R^\dagger{}_l$ =  . (1.8)

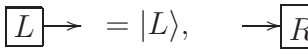
Needless to say, in the equation above, "l" is the index leaving the box on the left-hand-side, "r" the right-hand-side one. Connected lines designate contractions of the respective indices. Eq. (1.2) now reads

$\langle s_1, \ldots, s_n|\Psi\rangle =$ 

A single-index tensor can be interpreted as the expansion coefficients of either a "ket" or a "bra". Sometimes, we will indicate what interpretation we have in mind by placing

[2] These graphical formulae are compatible with various similar systems introduced before [27, 43].

arrows on the edges: outgoing arrows designating “kets”, incoming arrows “bras”



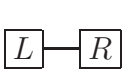
(1.9)

Tensors with two indices $A_{l,r}$ can naturally be interpreted as operators. In the graphical notation we often want to think of information flowing from the left to the right, in which case $A = \sum_{l,r} A_{l,r} |r\rangle_r \langle l|_l$ would be denoted as

(1.10)

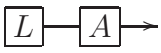
i.e. with the l.h.s. index being associated with a “bra” and the r.h.s one with a “ket”. The following relations exemplify the definition:

$\langle R|L\rangle$ =



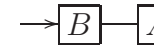
(1.11)

$A|L\rangle$ =



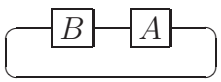
(1.12)

AB =



(1.13)

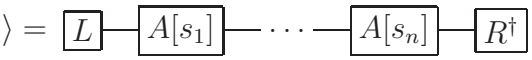
$\mathrm{tr}(AB)$ =



(1.14)

The formula for the expansion coefficients of a matrix product state finally becomes

$\langle s_1, \ldots, s_n|\Psi\rangle =$



This formula suggest a more “dynamic” interpretation of MPS: the l.h.s. boundary conditions $|L\rangle$ specify an initial state of the correlation system, which is acted on by the matrices of the MPS representation. The next paragraph is going to elaborate on this point.

1.2.2 Quantum computing in correlation systems

We return to the discussion of the properties of matrix product states. Above, it has been shown how to compute the overlap of $|\Psi\rangle$ with an element of the computational basis (c.f. Eq. (1.5)). The next step is to generalize this to any local projection operator. Indeed, if $|\phi\rangle$ is a general state vector in $\mathbb{C}^2$, we abbreviate

$$\langle\phi|0\rangle\, A[0] + \langle\phi|1\rangle\, A[1] =: A[\phi]. \tag{1.15}$$

One then easily derives the following, central formula

$$\Big(\bigotimes_i^n \langle\phi_i|\Big)|\Psi\rangle = \boxed{L}\!-\!\boxed{A[\phi_1]}\!-\cdots-\!\boxed{A[\phi_n]}\!-\!\boxed{R}\,. \tag{1.16}$$

Now suppose we measure local observables on $|\Psi\rangle$ and obtain results corresponding to the eigenvector $|\phi_i\rangle$ at the i-th site. Eq. (1.16) allows us to re-interpret this process as follows. Initially, the D-dimensional correlation system is prepared in the state $|L\rangle$. The result $|\phi_1\rangle$ at the first site induces the evolution

$$|L\rangle \mapsto A[\phi_1]|L\rangle. \tag{1.17}$$

From this point of view, a sequence of measurements on $|\Psi\rangle$ is tantamount to a processing of the correlation system's state by the operations $A[\phi_i]$.[3] An appealing perspective on MBC suggests itself:

Observation 3 (Role of correlation space)**.** *Measurement-based computing takes place in correlation space. The gates acting on the correlation systems are determined by local measurements. Intuitively, "quantum correlations" are the source of a resource's computational potency. The strength of this framework lies in the fact that it assigns a concrete mathematical object to these correlations.*

Indeed, it will turn out that MBQC can be understood completely using this interpretation.

[3] Of course, for general measurement bases, $A[\phi_i]$ is not going to be unitary. Choosing the bases in such a way as to ensure unitarity is an essential part of the design of a computational scheme for a given resource.

1.2.3 Example: The 1-D cluster state

To illustrate the abstract definitions made above, we will discuss the linear cluster state vector $|Cl_n\rangle$ in this section. It is both one of the simplest and certainly the most important MPS in the context of MBQC.

What is the tensor network representation of $|Cl_n\rangle$? Recall that the cluster state can be generated by preparing n sites in the state vector $|+\rangle := |0\rangle + |1\rangle$ and subsequently applying the controlled-Z operation

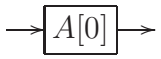
$$CZ = |0,0\rangle\langle 0,0| + |0,1\rangle\langle 0,1| + |1,0\rangle\langle 1,0| - |1,1\rangle\langle 1,1| \tag{1.18}$$

between any two nearest neighbors. Effectively, CZ introduces a π-phase whenever two consecutive systems are in the $|1\rangle$-state. Hence its expansion coefficients in the computational basis are given by

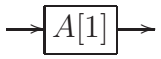
$$\langle s_1, \ldots, s_n | Cl_n \rangle = 2^{-n/2}(-1)^p, \tag{1.19}$$

where p denotes the number of sites i such that $s_i = s_{i+1} = 1$.

This observation makes it simple to derive the tensors of the MPS representation. We need a $D = 2$-dimensional correlation system, which – loosely speaking – will convey the information about the state s_i of the i-th site to site $i+1$. Define the matrices $A[0/1]$ by



$$= |+\rangle_r\langle 0|_l, \tag{1.20}$$



$$= |-\rangle_r\langle 1|_l. \tag{1.21}$$

The intuition behind this choice is as follows. By the elementary relations

$$\langle +|0\rangle = \langle +|1\rangle = \langle -|0\rangle = 2^{-1/2}, \qquad \langle -|1\rangle = -2^{-1/2}, \tag{1.22}$$

the contraction in the middle of

(1.23)

will yield a sign of "-1" exactly if $s_1 = s_2 = 1$. Indeed, setting the boundary vectors to $|L\rangle = |0\rangle, |R\rangle = |+\rangle$ one checks easily that

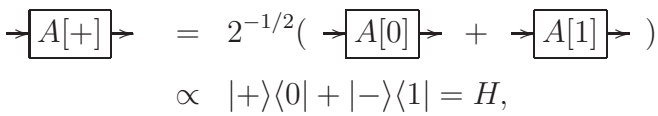
$$\langle R|A[s_n]\dots A[s_1]|L\rangle = 2^{-n/2}(-1)^p, \tag{1.24}$$

which is exactly the value required by Eq. (1.19).

Below, we will interpret the correlation system of a 1-D chain as a single logical quantum system. For this interpretation to be viable, we must check that the following basic operations can be performed deterministically by local measurements: i) prepare the correlation system in a known initial state, ii) transport that state along the chain (possibly subject to known unitary transformations) and iii) read out the final state.

To set the state of the correlation system to a definitive value, we measure some site – say the i-th – in the Z-eigenbasis. Throughout this work, we will choose the notation X, Y, and Z for the *Pauli operators*. Denote the measurement outcome by $z \in \{0, 1\}$. In case of $z = 0$, Eq. (1.20) tells us that the state of the correlation system to the right of the i-th site will be $|+\rangle$ (up to an unimportant phase). Likewise, a $z = 1$ outcome prepares the correlation system in $|-\rangle$, according to Eq. (1.21). It follows that we can use Z-measurements for preparation. How to cope with the intrinsic randomness of quantum measurements will concern us later.

Secondly, consider the operators



$$\propto \quad |+\rangle\langle 0| + |-\rangle\langle 1| = H, \tag{1.25}$$

(1.26)

where H is the Hadamard-gate. We see immediately that measurements in the X-eigenbasis give rise to a unitary evolution on the correlation space. Similarly, one can show that one can generate arbitrary local unitaries by appropriate measurements in the Y-Z plane.

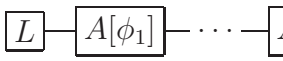
Below, we will frequently be confronted with a situation like the one presented in Eqs. (1.25,1.26), where the correlation system evolves in one of two possibilities, de-

pendent on the outcome of a measurement. It will be convenient to introduce a compact notation that encompasses both cases in a single equation. So Eqs. (1.25,1.26) will be represented as

(1.27)

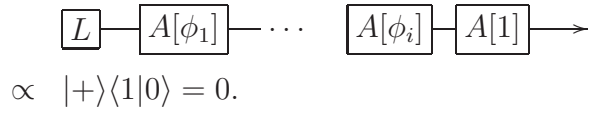
Here $x = 0$ corresponds to the outcome $|+\rangle$ in an X-measurement, whereas $x = 1$ corresponds to the outcome $|-\rangle$. In general, a physical observable given as an argument to a tensor corresponds to a measurement in the observable's eigenbasis. The measurement outcome is assigned to a suitable variable as in the above example.

Lastly, we must show how to physically read out the state of the purely logical correlation system. It turns out that measuring the $i+1$-th physical system in the Z-eigenbasis corresponds to a Z-measurement of the state of the correlation system just after site i. Indeed, suppose we have measured the first i systems and obtained results corresponding to the local projection operator $|\phi_1\rangle \otimes \cdots \otimes |\phi_i\rangle$. Further assume that as a result of these measurements the correlation system is in the state $|0\rangle$:



(1.28)

Using Eq. (1.21) we have that



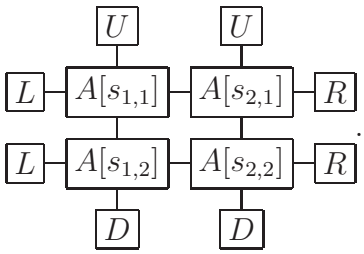
(1.29)

But then it follows from Eq. (1.16) that the probability of obtaining the result 1 for a Z-measurement on site $i+1$ is equal to zero. In other words: if the *correlation system* is in the state $|0\rangle$ after the i-th site, then the $i+1$-th *physical site* must also be in the state $|0\rangle$. An analogous argument for the $|1\rangle$-case completes the description of the read-out scheme.

1.2.4 2-D lattices

The graphical notation greatly facilitates the passage to 2-D lattices. Here, the tensors $A[s]$ have four indices $A[s]_{l,r,u,d}$, which will be contracted with the indices of the left,

right, upper and lower neighboring tensors respectively. After choosing a set of boundary conditions $|L\rangle, |R\rangle, |U\rangle, |D\rangle \in \mathbb{C}^D$, the expansion coefficients of the state vector $|\Psi\rangle$ are computed as illustrated in the following example on a 2×2-lattice:

$\langle s_{1,1}, \ldots, s_{2,2}|\Psi\rangle =$  . (1.30)

In the 1-D case, we thought of the quantum information as moving along a single correlation system from the left to the right. For higher-dimensional lattices, a greater deal of flexibility proves to be expedient. For example, sometimes it will be natural to interpret the tensor $A_{l,r,u,d}$ as specifying the matrix elements of an operator A mapping the left and the lower correlation systems to the right and the upper ones:

$$A_{l,r,u,d} = \langle r| \otimes \langle u| A |l\rangle \otimes |d\rangle, \quad A = \text{  .} \tag{1.31}$$

Often, on the other hand, the interpretation

$$A_{l,r,u,d} = \langle r| A |l\rangle \otimes |u\rangle \otimes |d\rangle, \quad A = \text{  } \tag{1.32}$$

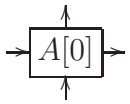
or yet another one is to be preferred.

We have seen in Section 1.2.2 that the correlation system of a one-dimensional matrix product state can naturally be interpreted as a single quantum system subject to a time evolution induced by local measurements. It would be desirable to carry this intuition over to the 2-D case. Indeed, most of the examples to be discussed below are all similar in relying on the same basic scenario: some horizontal lines in the lattice are interpreted as effectively one-dimensional systems, in which the logical qubits travel from the left to the right. The vertical dimension is used to either couple the logical systems or isolate them from each other. The reader should recall that this setting is very similar to the original cluster state based-techniques. Clearly, it would be interesting to devise

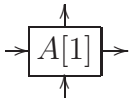
schemes not working in this way and the example presented in Section 1.3.2 takes a first step in this direction.

1.2.5 Example: the 2-D cluster state

Once again the cluster state serves as an example. One can work out the tensor network representation of the 2-D cluster state vector $|Cl_{n\times n}\rangle$ in the same way utilized for the 1-D case in Section 1.2.3. The resulting tensors are:



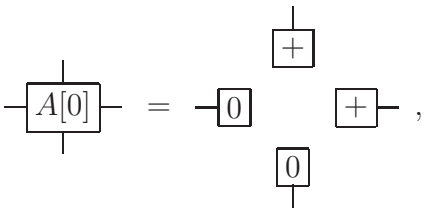
$$= |+\rangle_r |+\rangle_u \langle 0|_l \langle 0|_d, \tag{1.33}$$



$$= |-\rangle_r |-\rangle_u \langle 1|_l \langle 1|_d, \tag{1.34}$$

$$|L\rangle = |D\rangle = |+\rangle, \qquad |R\rangle = |U\rangle = |1\rangle. \tag{1.35}$$

An important property of Eqs. (1.33, 1.34) is that the tensors $A[0/1]$ factor. One could graphically represent this fact by writing



, (1.36)

where

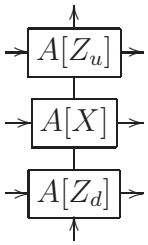
$= |0\rangle,$

$= |+\rangle.$ (1.37)

In other words: the tensors $A[0/1]$ effectively de-couple their respective indices. Based on this fact, we will see momentarily how Z-measurements can be used to stop information from flowing through the lattice.

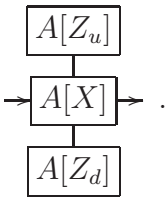
Indeed, suppose three vertically adjacent sites are measured, from top to bottom,

respectively in the Z, X and Z-eigenbasis:



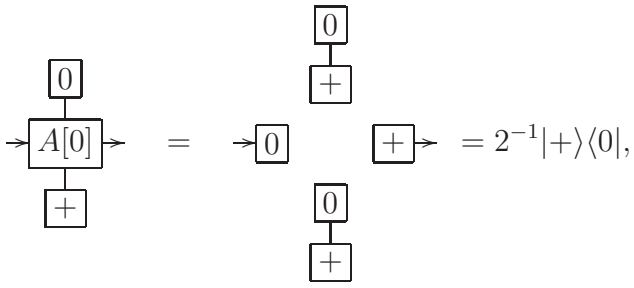
. (1.38)

Denote the measurement results by $z_u, x, z_d \in \{0, 1\}$. As before, these numbers correspond to $z_u = 0$ for $|0\rangle$ and $z_u = 1$ for $|1\rangle$, as well as $x = 0$ for $|+\rangle$ and $x = 1$ for $|-\rangle$. In fact, we are mainly interested in the indices of the middle tensor, as they will be the ones which carry the logical information. To this end Eq. (1.36) is of use, as it says that the upper and lower tensors factor and hence it makes sense to dis-regard all of their indices which do not influence the middle part. It hence suffices to consider



. (1.39)

As a first step, we calculate

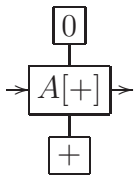


having used Eq. (1.36) and the basic fact

$= \langle 0|+\rangle = 2^{-1/2}.$ (1.40)

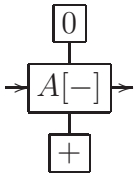
A similar calculation where $A[0]$ is substituted by $A[1]$ yields $2^{-1}|-\rangle\langle 1|$. Hence, for

$A[+] \propto A[0] + A[1]$, we have



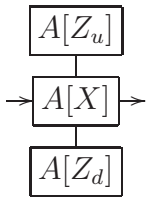
$$\propto \quad |+\rangle\langle 0| + |-\rangle\langle 1| = H. \tag{1.41}$$

Similarly,



$$\propto \quad HZ. \tag{1.42}$$

After these preparations it is simple to conclude that



$$\propto HZ^{z_u+x+z_d}. \tag{1.43}$$

This finding tells us how to transport quantum information along horizontal lines through the lattice. Namely by measuring the line in the X-eigenbasis to cause the information to flow from the left to the right and measuring vertically adjacent sites in the Z-eigenbasis to shield the information from the rest of the lattice.

Eq. (1.43) should be compared with Eqs. (1.25,1.26). So up to possible corrections of the form $Z^{z_u+z_l}$, the procedure outlined above enables us to effectively prepare a 1-D cluster state within the 2-D lattice.

1.3 Novel resource states

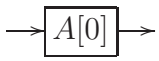
Up to this point, we have reformulated the computational model of the one-way computer in the language of computational tensor networks. This picture of one-way computation is educational in its own right. However, to convincingly argue that the framework is rich enough to allow for quite different models, we have to explicitly construct novel schemes. It is the purpose of this section to discuss a number of examples of new

resources. As before, important features will be highlighted as “observations”.

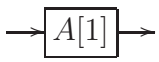
1.3.1 AKLT-type states

1-D structures

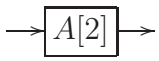
Our first example is inspired by the *AKLT state* [2], which is well-known in the context of condensed matter physics. The *AKLT model* is a 1-D, spin-1, nearest neighbor, frustration free, gapped Hamiltonian. Its unique ground state is a matrix product state with $D = 2$ and indeed, the AKLT model motivated the first studies of such states [2, 35]. The defining matrices of the MPS description are:



$$= Z, \tag{1.44}$$

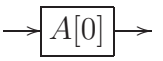


$$= 2^{-1/2}|0\rangle_r\langle 1|_l, \tag{1.45}$$



$$= 2^{-1/2}|1\rangle_r\langle 0|_l \tag{1.46}$$

We will choose the boundary conditions to be $|L\rangle = |R\rangle = |0\rangle$. As a matter of fact, we will not work directly with the AKLT state, but with a small variation, for which it turns out to be more straight-forward to construct a scheme for MBQC. In this modification, the matrix $A[0]$ is given by the Hadamard gate, instead of the Pauli Z operator:



$$= H. \tag{1.47}$$

This state shares all the defining properties of the original: it is the unique ground-state of a spin-1 nearest neighbor frustration free gapped Hamiltonian (see Appendix 1.6.2). Against the background of our program, the obvious question to ask is whether these matrices can be used to implement any evolution on the correlation space.

To show that this is indeed the case, let us first analyze a measurement in the $\{|0\rangle, |+\rangle, |-\rangle\}$-basis, where $|\pm\rangle := 2^{-1/2}(|1\rangle \pm |2\rangle)$. In a mild abuse of notation, we will hence write $|\pm\rangle$ for state vectors in the subspace spanned by $\{|1\rangle, |2\rangle\}$ instead of $\{|0\rangle, |1\rangle\}$. From Eqs. (1.44-1.47) one finds that depending on the measurement outcome, the operation realized on the correlation space will be one of H, X or $ZX = iY$. At this point, we have to turn to an important issue: how to compensate for the random-

ness of quantum measurement outcomes.

Compensating the randomness

Assume for now that we intended to just transport the information faithfully from left to right. In this case, we consider the operator

$$B_1 := H, X, \text{ or } ZX \tag{1.48}$$

as an unwanted *by-product* of the scheme. The one-way computer based on cluster states has the remarkable property that the by-products can be dealt with by adjusting the measurement-bases depending on the previous outcomes, without changing the general "layout" of the computation [90]. For more general models, as the ones considered in this work, such a simple solution seems not available. Fortunately, we can employ a "trial-until-success" strategy, which proves remarkably general.

The key points to notice are that i) the three possible outcomes H, X and Z generate a finite group $\mathcal{B}$ and ii) the probability for each outcome is equal to $1/3$, independent of the state of the correlation system. We will refer to $\mathcal{B}$ as the model's *by-product* group. Now suppose we measure m adjacent sites in the $\{|0\rangle, |+\rangle, |-\rangle\}$-basis. The resulting overall by-product operator $B = B_m B_{m-1} \dots B_1$ will be a product of m generators H, X, ZX. So by repeatedly transporting the state of the correlation system to the right, the by-products are subject to a random walk on $\mathcal{B}$. Because $\mathcal{B}$ is finite, every element will occur after a finite expected number of steps (as one can easily prove).

The group structure opens up a way of dealing with the randomness. Indeed, assume that initially the state vector of the correlation system is given by $B|\psi\rangle$, for some unwanted $B \in \mathcal{B}$. Transferring the state along the chain will introduce the additional by-product operator B^{-1} after some finite expected number of steps, leaving us with

$$B^{-1}B|\psi\rangle = |\psi\rangle, \tag{1.49}$$

as desired. The technique outlined here proves to be extremely general and we will encounter it in further examples presented below.

Observation 4 (Compensating randomness)**.** *Possible sets of by-product operators are*

not limited to the Pauli group. A way of compensating randomness for other finite by-product operator groups is to adopt a "trial-until-success strategy", which gives rise to a random length of the computation. This length is in each case shown to be bounded on average by a constant in the system size.

All single-qubit gates

By the preceding paragraphs, we can implement any element of $\mathcal{B}$ on the correlation space. We next address the problem of realizing a phase gate $S(\phi) := \mathrm{diag}(1, e^{i\phi})$ for some $\phi \in \mathbb{R}$. To this end, consider a measurement on the $\{|0\rangle, 2^{-1/2}(|1\rangle \pm e^{i\phi}|2\rangle)\}$-basis. There are three cases

- The outcome corresponds to $|1\rangle + e^{i\phi}|2\rangle$. In this case, we get $S(\phi)$ on the correlation space and are hence done.
- The outcome corresponds to $|1\rangle - e^{i\phi}|2\rangle$. We get $ZS(\phi)$, which is the desired operation, up to an element of the by-product group, which we can rid ourselves of as described above.
- Lastly, in case of $|0\rangle$, we implement H on the correlation space. As $H \in \mathcal{B}$, we can "undo" it and then re-try to implement the phase gate.

Hence, we can implement any element of $\mathcal{B}$ as well as $S(\phi)$ on the correlation space. This implies that $HS(\phi)H$ is also realizable and therefore any single-qubit unitary, as $SU(2)$ is generated by operations of the form $S(\phi)$ and $HS(\phi)H$.

The state of the correlation system can be prepared by measuring in the computational basis. In case one obtains a result of "1" or "2", the state of the correlation system will be $|0\rangle$ or $|1\rangle$ respectively, irrespective of its previous state. A "0"-outcome will not leave the correlation system in a definite state. However, after a finite expected number of steps, a measurement will give a non-"0"-result. Lastly, a read-out scheme can be realized similarly (c.f. Section 1.2.3).

Observation 5 (Ground states)**.** *Ground states of one-dimensional gapped nearest-neighbor Hamiltonians may serve as resources for transport and arbitrary rotations.*

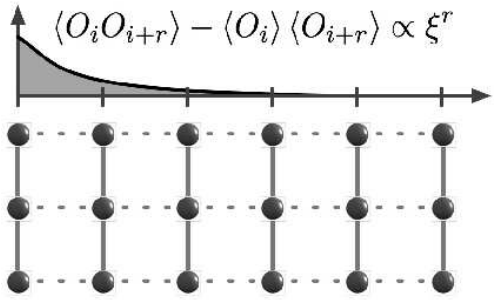
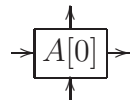


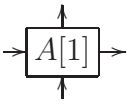
Figure 1.1: A universal resource deriving from the AKLT-model.

2-D structures

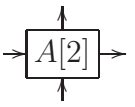
Several horizontal 1-D AKLT-type states can be coupled to become a universal 2-D resource. The coupling can be facilitated by performing a controlled-Z operation, embedded into the three-dimensional spin-1 space, between vertically adjacent nearest neighbors. More specifically, we will use the operation $\exp\{i\pi|2\rangle\langle 2|\otimes|2\rangle\langle 2|\}$, which introduces a π-phase between two systems exactly if both are in the state $|2\rangle$. The tensor network representation of this resource is given by



$$= H_{l\to r}\otimes|+\rangle_u\langle 0|_d, \tag{1.50}$$



$$= 2^{-1/2}|0\rangle_r\langle 1|_l\otimes|+\rangle_u\langle 0|_d, \tag{1.51}$$



$$= 2^{-1/2}|1\rangle_r\langle 0|_l\otimes|-\rangle_u\langle 1|_d, \tag{1.52}$$

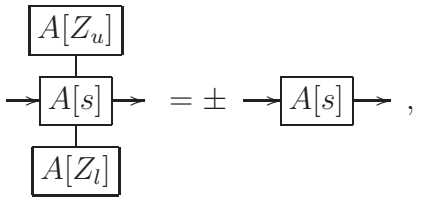
as one can check in analogy to Sec. 1.2.5. Here,

$$H_{l\to r} := |+\rangle_r\langle 0|_l + |-\rangle_r\langle 1|_l. \tag{1.53}$$

To verify that the resulting 2-D state constitutes a universal resource, we need to check that a) one can isolate the correlation system of a horizontal line from the rest of the lattice, so that it may be interpreted as a logical qubit and b) one can couple these

logical qubits to perform an entangling gate.

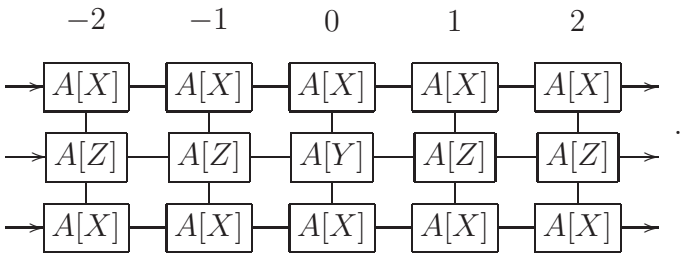
The first step works in complete analogy to Section 1.2.5, see Fig. 1.1. Indeed, one simply confirms that



(1.54)

where $s \in \{0,1,2\}$ and $Z_{u/l}$ denotes a measurement in the $\{|0\rangle, |1\rangle, |2\rangle\}$-basis. So measuring the vertically adjacent nodes in the computational basis gives us back the 1-D state, up to a possible sign.

A controlled-Z gate can be realized in five steps:

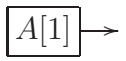


(1.55)

The Pauli matrices X, Y, Z are understood as being embedded into the $\{|1\rangle, |2\rangle\}$-subspace. So, e.g., X denotes a measurement in the $\{|0\rangle, 2^{-1/2}(|1\rangle \pm |2\rangle)\}$-basis. When operating the gate, we first measure all sites of the upper and lower lines in the X-eigenbasis. In case the result for the sites at position "0" (refer to labeling above) is different from $|+\rangle$, the gate failed. In that case all sites on the middle line are measured in the computational basis and we restart the procedure five steps to the right[4]. Otherwise, the systems labeled by a Z are measured. We accept the outcome only if we obtained $|1\rangle$ on sites ± 2 and $|0\rangle$ on sites ± 1 – should a different result occur, the gate is once again considered a failure and we proceed as above. Lastly, the Y measurement on the central site is performed. In case of a result corresponding to $|0\rangle$, it is easy to see that no interaction between the upper and the lower part takes place, so this is the last possibility for the

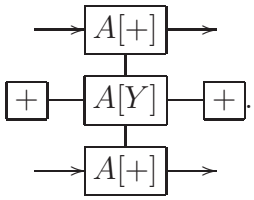
[4]We have chosen this approach in order to avoid an awkward discussion of how to handle phases introduced by "wrong" measurement outcomes. We are providing proofs of principle for universality here and will accept a (possibly daunting) linear overhead in the expected number of steps, if this simplifies the discussion. Substantial improvements to these schemes are, of course, possible.

gate to fail. Let us assume now that the desired measurement outcomes were realized. At site -2 on the middle line, we obtained



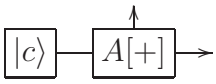
(1.56)

which prepares the correlation system of the middle line in $|0\rangle$. At site -1, in turn, a Hadamard gate has been realized, which causes the output of site -1 to be $H|0\rangle = |+\rangle$. The situation is similar on the r.h.s., so that the above network at site 0 can be re-written as



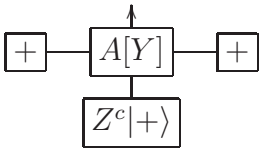
(1.57)

We will now analyze the tensor network in Eq. (1.57) step by step. For proving its functionality, there is no loss of generality in restricting attention to the situation where the correlation system of the lower line is initially in state $|c\rangle$, for $c \in \{0, 1\}$. We compute for the lower part of the tensor network



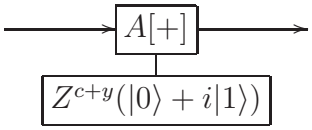
$= X|c\rangle_r Z^c|+\rangle_u.$ (1.58)

Further, plugging the output $Z^c|+\rangle$ of the lower stage into the middle part, we find



$\propto Z^{c+y}(|0\rangle + i|1\rangle),$ (1.59)

where $y \in 0, 1$ reflects the outcome of the Y-measurement on the central site: $y = 0$ in case of $|1\rangle + i|2\rangle$ and $y = 1$ for $|1\rangle - i|2\rangle$. Lastly,



$\propto SZ^{c+y}X.$ (1.60)

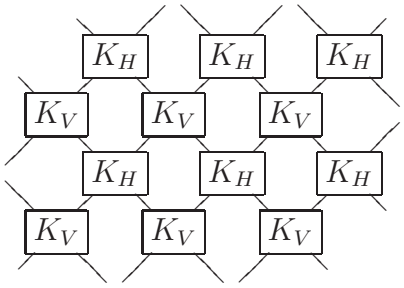
In summary, the evolution afforded on the upper line is HSZ^{y+c}, equivalent to Z^c up to by-products. This completes the proof of universality.

For completeness, note that we never need the by-products to vanish for all logical qubits of the full computation simultaneously. Hence the expected number of steps for the realization of one- or two-qubit gates is a constant in the number of total logical qubits.

1.3.2 Toric code states

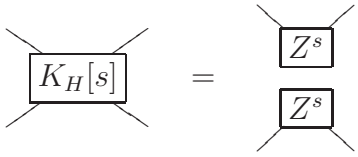
In the following, we present two MBQC resource states which are motivated by Kitaev's toric code states [70]. This contrasts with a result in Ref. [14] that MBQC on the planar toric code state itself can be simulated efficiently classically. Different from the other schemes presented, the natural gate in these schemes is a two-qubit interaction, whereas local operations have to be implemented indirectly. Also, individual qubits are decoupled not by erasing sites but by switching off the coupling between them.

Toric code states are states with non-trivial topological properties and have been introduced in the context of quantum error correction. They have a particularly simple representation in terms of PEPS [114] or CTNs [6] on two centered square lattices,



(1.61)

where



(1.62)

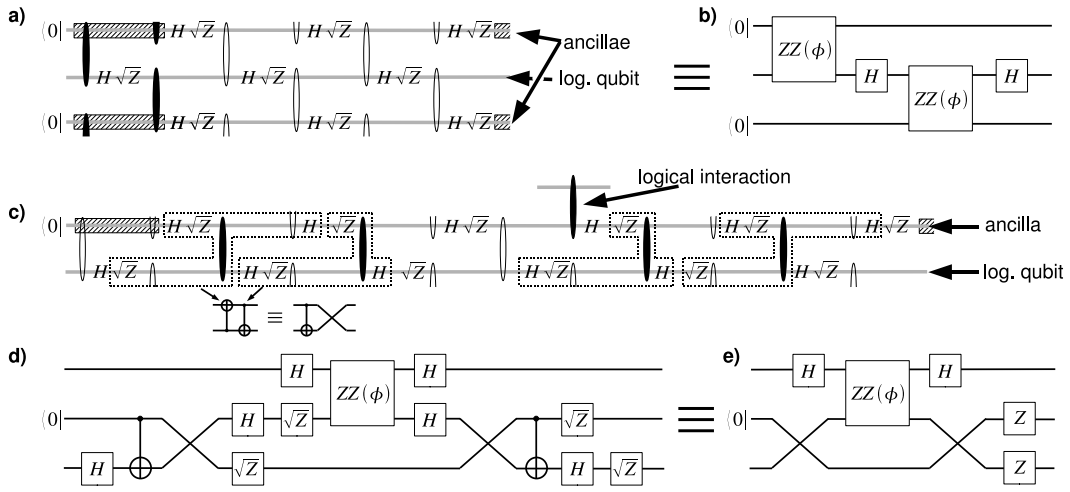
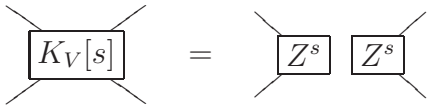


Figure 1.2: Implementation of single-qubit and two-qubit operations in the first toric code model. **a)** The measurement pattern for single-qubit operations and **b)** the corresponding circuit. **c)** Pattern for a two-qubit gate between logical qubits, **d)** the corresponding circuit and **e)** the circuit after some simplifications.

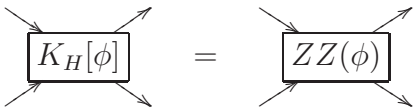
and



(1.63)

i.e., K_H and K_V are identical up to a rotation by 90 degrees.

Let us first see how K_H acts on two qubits in correlation space coming from the left. The most basic operation is a measurement in the computational basis, which simply transports both qubits to the right (up to a correlated Z by-product operator). Generalizing this to measurements in the Y-Z plane, we find that



(1.64)

where ϕ is the angle with the Z axis, and

$$ZZ(\phi) = \begin{pmatrix} 1 & & & \\ & e^{i\phi} & & \\ & & e^{i\phi} & \\ & & & 1 \end{pmatrix} . \tag{1.65}$$

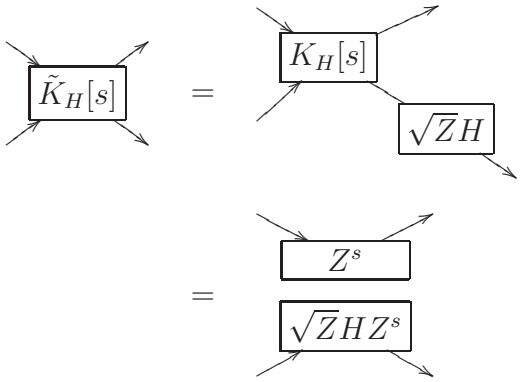
(Note that this gate is locally equivalent to the CNOT gate for $\phi = \pm\pi/2$.)

Thus, the tensors in Kitaev's toric code state have a *two*-qubit operation as their natural gate in correlation space, rather than a *single*-qubit gate. In MBQC schemes which base on these projectors, two-qubit gates are easy to realize, whereas in order to get one-qubit gates, tricks have to be used. In the first example, we obtain single-qubit operations by introducing ancillae: a ZZ controlled phase between a logical qubit and an ancilla in a computational basis state yields a local Z rotation on the logical qubit. In the second example, we use a different approach: we encode each logical qubit in *two* qubits in correlation space. Using this nonlocal encoding, we obtain an easy implementation of both one- and two-qubit operations; furthermore, the scheme allows for an arbitrary parallelization of the two-qubit interactions.

Observation 6 (Logical qubits in several correlation systems)**.** *There is no need to have a one-one correspondance between logical qubits and a single correlation system.*

Toric codes: first scheme

Our first scheme consists of the modified tensor



(1.66)

[with $\sqrt{Z} = \mathrm{diag}(1, i)$], arranged as in (1.61) where *both* K_H and K_V are replaced by $\tilde{K}_H$. The extra H serves the same purpose as in other schemes: it allows to leave the subspace of diagonal operations and thus to implement X rotations. The need for the $\sqrt{Z}$ will become clear later; it is connected to the fact that

$$\textsc{cnot} = (\mathbb{1} \otimes H)\ (\sqrt{Z} \otimes \sqrt{Z})\ ZZ(-\pi/2)\ (\mathbb{1} \otimes H)\ . \tag{1.67}$$

In the following, we show how this state can be used for MBQC. The qubits run from left to right in correlation space in zig-zag lines in Eq. (1.61); for the illustration in Fig. 1.2, we have straightened these lines, and marked the measurement-induced ZZ interactions coming from the $K_H[s]$ in (1.66) by ellipses. (The difference between filled and non-filled ellipses will be explained later.) The $\sqrt{Z}H$ operations of (1.66) do not depend on the measurement and are thus hard-wired; note that the order is reversed as we are considering H and $\sqrt{Z}$ as two independent operations in the circuit.

Let us first impose that all qubits are initialized to $|0\rangle$; this corresponds to a left boundary condition $|0\rangle$ in correlation space. We will discuss later how to initialize the scheme. Every second qubit is an ancilla which will be used to implement one-qubit operations. We first discuss the case of no Pauli errors, and show later how those can be dealt with.

The implementation of single-qubit operations is illustrated in Fig. 1.2a. There, each ellipse denotes a possible ZZ interaction. In particular, empty ellipses denote interactions which are switched off (i.e. measured in the Z basis), while filled ellipses denote sites where one can measure in the Y-Z plane to implement a ZZ gate. If all interactions are switched off, all qubits are transported to the right, subject to the transformation $\sqrt{Z}H$. As $(\sqrt{Z}H)^3 = \mathbb{1}$, the ancillae are in the computational basis in every third step: These regions are hashed in Fig. 1.2a. In these regions, a $ZZ(\phi)$ between ancilla and logical qubit (corresponding to the filled ellipses in the figure) results in a single-qubit Z rotation on the latter. Thus, in each block of length three as the one shown in Fig. 1.2a, the transformation

$$\sqrt{Z}H\sqrt{Z}HS(\psi)\sqrt{Z}HS(\phi) = HS(\psi)HS(\phi) \tag{1.68}$$

is implemented [where $S(\phi) = \mathrm{diag}(1, e^{i\phi})$], which allows for arbitrary one-qubit operations. In Fig. 1.2b, the corresponding circuit is shown, which has been simplified using $H\sqrt{Z}H\sqrt{Z} = \sqrt{X}\sqrt{Z} = (\sqrt{Z})^{-1}H$, and that diagonal matrices commute.

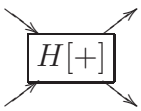
Although the scheme has a natural two-qubit interaction, implementing an interaction between two adjacent *logical* qubits is complicated by the ancilla which is located inbetween. In order to obtain a coupling, we first swap the logical qubit with the ancilla, then couple it to the now adjacent logical neighbor, and finally swap it back. This is implemented by the measurement pattern shown in Fig. 1.2c. Again, empty ellipses correspond to switched off interactions, while the filled ellipses all implement $ZZ(-\pi/2)$ gates, each of which together with two $\sqrt{Z}$ and two Hadamards as grouped in the figure gives a CNOT gate, cf. Eq. (1.67). This measurement pattern corresponds to the circuit shown in Fig. 1.2d, where we have replaced each pair of CNOTs by a CNOT and a SWAP. By merging each CNOT with the two adjacent Hadamards, we effectively obtain

$$CZ = |0,0\rangle\langle 0,0| + |0,1\rangle\langle 0,1| + |1,0\rangle\langle 1,0| - |1,1\rangle\langle 1,1| \tag{1.69}$$

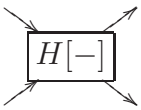
gates. We thus remain with only diagonal gates on the two lower qubits (except for the SWAP), i.e. the gates all commute and the circuit can thus be simplified to the one shown on in Fig. 1.2e, proving that the sequence effectively implements a two-qubit interaction between the logical qubits. Note that the length of the complete sequence is compatible with the three-periodicity of the basis of the ancillae.

Pauli errors in this scheme can be dealt with as usual: H and $\sqrt{Z}$ are both in the Clifford group, i.e., Paulis can be commuted through, and ZZ commutes with Z errors, while $(\mathbb{1} \otimes X)ZZ(\phi) = ZZ(-\phi)(\mathbb{1} \otimes X)$.

Finally, we show how to read out the logical qubits. It holds that



$$= \left|\begin{matrix}0\\0\end{matrix}\right\rangle\left\langle\begin{matrix}0\\0\end{matrix}\right| + \left|\begin{matrix}1\\1\end{matrix}\right\rangle\left\langle\begin{matrix}1\\1\end{matrix}\right|, \tag{1.70}$$



$$= \left|\begin{matrix}0\\1\end{matrix}\right\rangle\left\langle\begin{matrix}0\\1\end{matrix}\right| + \left|\begin{matrix}1\\0\end{matrix}\right\rangle\left\langle\begin{matrix}1\\0\end{matrix}\right|, \tag{1.71}$$

i.e., a measurement in the X basis returns the parity of the ancilla and the logical qubit.

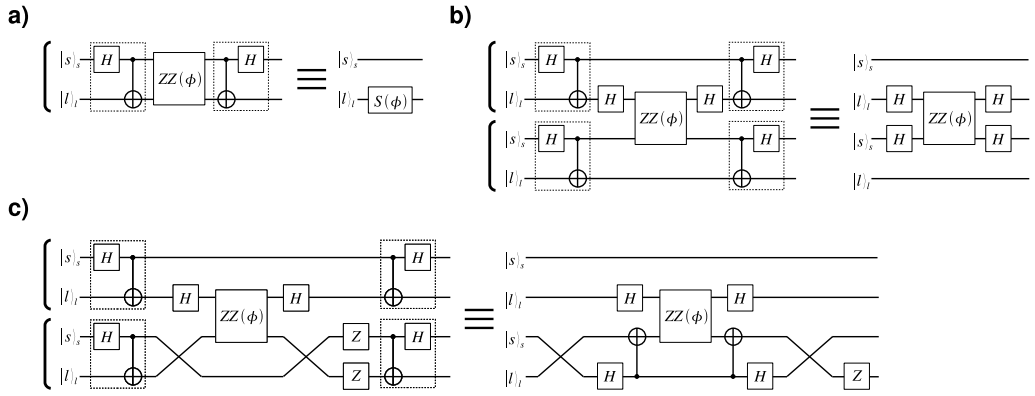


Figure 1.3: Interpretation of the first toric code scheme in terms of parity encoded qubits. The boxed parts of the circuit decode and encode the system. **a)** Z rotations result in Z rotations in the encoded system. **b)** X rotations result in X rotations in the encoded system, plus Z corrections before and after the rotations in case the s qubit below is $|-\rangle_s$ rather than $|+\rangle_s$. **c)** Similarly, the coupling circuit Fig. 1.2d results in a coupling of the encoded logical qubits, up to the same Z correction on the first logical qubit which depends on the s qubit below in exactly the same way. Thus, the Z corrections on each qubit cancel out except for the first and the last, which have no effect due to the initialization and measurement in the computational basis.

If this is done when the ancilla is in a computational basis state, one effectively measures the logical qubit in the computational basis. Note that both the ancilla and the logical qubit are in a well-defined state afterwards and can thus be reused.

Let us now turn towards the initialization procedure. In contrast to the previous MBQC schemes, the read-out cannot be used for initialization. The reason is that the read-out only works if the ancilla qubit is initially in a computational basis state; otherwise, it just projects onto the subspace spanned by $\{|0,0\rangle, |1,1\rangle\}$ or by $\{|0,1\rangle, |1,0\rangle\}$.

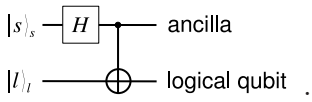
In the following, we demonstrate that it is still possible to initialize this scheme by taking a different perspective on how it encodes logical qubits. Therefore, we group each logical qubit with the ancilla above (e.g., the first two qubits in Fig. 1.2a), and encode the new logical qubit in their parity – note that this is what is really measured in the read-out. The following calculations are most conveniently carried out in a Bell basis where each state is described as $|s\rangle_s|l\rangle_l$, where the s qubit stores the sign of the

Bell state and the l qubit the parity and thus encodes our logical qubit, i.e.

$$|s\rangle_s|0\rangle_l \quad \leftrightarrow \quad |0,0\rangle + (-1)^s|1,1\rangle \tag{1.72}$$

$$|s\rangle_s|1\rangle_l \quad \leftrightarrow \quad |0,1\rangle + (-1)^s|1,0\rangle \; . \tag{1.73}$$

The circuit transforming between the above encoding and the qubits in correlation space is



. (1.74)

Using this decoding, it is straightforward to investigate what happens in the various steps of the MBQC scheme. Firstly, one can easily check that by measuring two consecutive couplings of the qubit pair in the X basis, one prepares them in a maximally entangled state $|0,0\rangle + |1,1\rangle$ up to Pauli errors, corresponding to $|0\rangle_s|0\rangle_l$ in the encoded system. By pretending a Pauli Z error on one of the qubits with $p = 1/2$, we effectively face the mixture $|0,0\rangle\langle 0,0| + |1,1\rangle\langle 1,1|$, corresponding to $\mathbb{1}_s \otimes |0\rangle\langle 0|_l$.

Since the transformation (1.74) is in the Clifford group, Pauli errors remain Pauli errors in the encoded system. In the following, we will check how the circuit acts on initial states $|\pm\rangle_s|0\rangle_l$, where the sign can be different on each pair. As we will show, all of them give the same output statistics, and thus the same holds for their mixture, i.e. the actual initial state. These considerations are illustrated in Fig. 1.3, where we take the circuits of Fig. 1.2 and compose them with the decoding and encoding circuits (boxed) in order to determine their action on the encoded system.

Firstly, a $ZZ(\phi)$ gate on a pair gives a Z rotation of the encoded logical qubit, since the action of $ZZ(\phi)$ only depends on the parity (Fig. 1.3a). The action of the second ZZ rotation of Fig. 1.2b which originally gave an X rotation is shown in Fig. 1.3b. The right hand side is obtained by using $\text{CNOT} = (\mathbb{1} \otimes H)\, CZ\, (\mathbb{1} \otimes H)$, $H^2 = \mathbb{1}$, the fact that diagonal operators commute, and $(CZ)^2 = \mathbb{1}$. As we see from the simplified circuit, we obtain an X rotation on the upper logical qubit, but with the rotation direction determined by the state of the $|s\rangle_s$ qubit below: While $|+\rangle_s$ results in a rotation $R_x(\phi)$, the state $|-\rangle_s$ gives

$$ZR_x(\phi)Z \propto R_x(-\phi) \; .$$

Similarly, the circuit for the coupling of two logical qubits can be simplified as in Fig. 1.3c: again, the coupling on the logical qubits is $\mathrm{Cpl}(\phi) := (H \otimes Z)ZZ(\phi)(H \otimes \mathbb{1})$ or

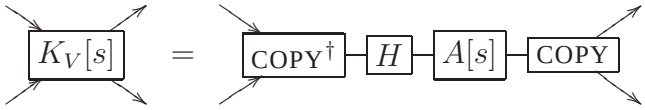
$$(H \otimes ZX)ZZ(\phi)(H \otimes X) = (Z \otimes \mathbb{1})\mathrm{Cpl}(\phi)(Z \otimes \mathbb{1}) \,,$$

depending on whether the second s qubit is $|+\rangle_s$ or $|-\rangle_s$.

Therefore, the error introduced by the unknown state of each s qubit results in a Z correction around each operation on the logical qubit above (note that we can assume this also for Z rotations as they commute with the Z correction). Although the error itself is unknown and different for each logical qubit, it is consistent within each qubit, as it is always determined by the same ancilla. Thus, two subsequent Z errors cancel out, and one remains only with one Z correction on the logical qubit at the beginning and one at the end of the sequence. The former has no effect since the initial state is $|0\rangle_l$, while the latter has no effect either since the encoded logical qubit is finally measured in the computational basis. Thus, the output statistics for the circuit is independent of the initial state $|\pm\rangle_s$ of the phase qubits, and one can equally well start from their mixture $\mathbb{1}_s$ which completes the argument.

Toric codes: second scheme

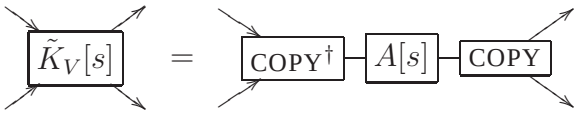
The second toric-code-like scheme is based on a very different idea. Therefore, observe that the K_V tensor can be written as



(1.75)

where COPY is the copy gate $|0,0\rangle\langle 0| + |1,1\rangle\langle 1|$, H is the Hadamard gate (both with no physical system associated to them), and A the 1-D cluster projector, cf. Eqs. (1.20) and (1.21). Thus, K_V takes two qubits in correlation space, projects them onto the $\{|0,0\rangle, |1,1\rangle\}$ subspace, implements the 1-D cluster map up to a Hadamard, and duplicates the output to two qubits. Concatenating these tensors horizontally [this takes place in (1.61) if all K_H's are measured in Z, and one neglects Pauli errors] therefore implements a single logical qubit line, encoded in two qubits in correlation space. By

removing the Hadamard gate from K_V, we obtain a 1-D cluster state encoded in two qubits which is thus capable of implementing any one-qubit operation on the logical qubit; in particular, this includes intialization and read-out. We thus define the tensor



. (1.76)

Then, the toric code state (1.61) with K_V replaced by $\tilde{K}_V$ is universal for MBQC: Initialization, one-qubit operations, and read-out are done exacly as in the 1-D cluster state. The logical qubits are decoupled up to Z by-product operators in correlation space by measuring the K_H tensors in the Z basis. The Z by-products in correlation space correspond to Z errors on the encoded logical qubits and thus can again be dealt with as in the cluster. In order to couple two logical qubits, we measure a K_H tensor in the Y basis and obtain a ZZ controlled phase gate in correlation space, which translates to the same gate on the logical qubits. Note that this model has the additional feature that as as many controlled phases (between nearest neighbors) as desired can be implemented simultaneously.

In the light of the discussion on the initialization of the first scheme, one might see similarities between the two schemes, since in both cases the information is effectively encoded in pairs of qubits. Note however that in the first scheme, the information is stored in the parity of the two qubits, and the full 4-dimensional space is being used; the reason for this encoding came from the properties of the K_H tensor used as a map in horizontal direction. In contrast, the second scheme only populates the 2-dimensional even parity subspace, and the qubit is rather stored in two copies of the same state; finally, the encoding is motivated by the properties of the K_V tensor as a map on correlation space in horizontal direction.

1.3.3 Weighted graph states

In this section, we will consider instances of *weighted graph states* [31, 54] forming universal resources. To motivate the construction, recall that the cluster state can be

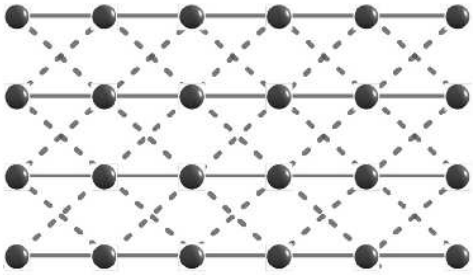


Figure 1.4: Weighted graph state as a universal resource. Solid lines correspond to edges that have been entangled using phase gates with phase $\phi = \pi$, dotted lines correspond to edges entangled with phase gates with $\phi = \pi/2$. This shows that one can replace some edges with weakly entangled bonds.

prepared by applying a controlled-phase gate

$$P(\phi) = |0,0\rangle\langle 0,0| + |0,1\rangle\langle 0,1| + |1,0\rangle\langle 1,0| + e^{i\phi}|1,1\rangle\langle 1,1|, \tag{1.77}$$

with phase $\phi = \pi$ between any two nearest neighbors of a two-dimensional lattice of qubits initially in the state $|+\rangle$. If one wants to physically implement this operation using *linear optics* [32], one encounters the situation that the controlled phase gate can be implemented only probabilistically, with the probability of success decreasing as ϕ increases. It is hence natural to ask whether one can build a universal resource using gates $P(\phi), 0 < \phi < \pi$, in order to minimize the probability of failure[5]

Translationally invariant weighted graph states

Expanding the discussion presented in Ref. [6], we treat the weighted graph state shown in Fig. 1.4. A tensor network representation of these states can be derived along the same lines as for the original cluster in Section 1.2.3. Set $|i\rangle := 2^{-1/2}(|0\rangle + i|1\rangle)$. The

[5]Alternative models with edges resulting from commuting gates with non-maximally entangling power can possibly also be constructed by exploiting ideas of non-local gates that are implemented with local operations and classical communication [25, 26, 33, 111].

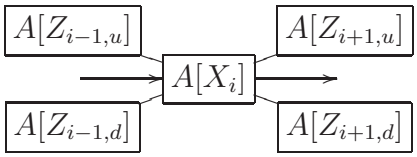
relevant tensors are given by

$$= |+\rangle_{ru} |+\rangle_{lu} |+\rangle_{r} \langle 0|_{ld} \langle 0|_{rd} \langle 0|_{l}, \tag{1.78}$$

$$= |i\rangle_{ru} |i\rangle_{lu} |-\rangle_{r} \langle 1|_{ld} \langle 1|_{rd} \langle 1|_{l}. \tag{1.79}$$

Indices are labeled ru for "right-up" to ld for "left-down". The boundary conditions are $|0\rangle$ for the ru, lu, r-directions; $|+\rangle$ otherwise.

We will first describe how to realize isolated evolutions of single logical qubits. Again the strategy will be to measure the sites of one horizontal line of the lattice in the X-basis and all vertically adjacent systems in the Z-basis. The analysis of the situation proceeds in perfect analogy to the one given in Section 1.2.5. One obtains



$$= HS^{2x_i + z_i}, \tag{1.80}$$

where

$$z_i = z_{i-1,u} + z_{i-1,d} + z_{i+1,u} + z_{i+1,d}, \tag{1.81}$$

and $S := \mathrm{diag}(1, i)$ denotes the $\pi/4$ *gate*.

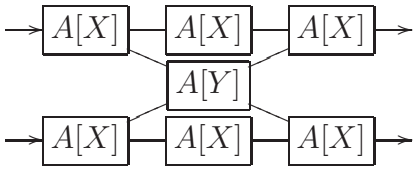
The operators H and S generate the 24-element single qubit Clifford group. Following the approach of Section 1.3.1, we take this as the model's by-product group.

Now choose some phase ϕ. Re-doing the calculation which led to Eq. (1.80), where we now measure in the $\{|0\rangle \pm e^{i\phi}|1\rangle\}$-basis instead of X on the central node, shows that the evolution of the correlation space is given by $S(\phi)$, up to by-products. In complete analogy to Section 1.3.1, we see that the model allows for the realization of arbitrary $SU(2)$ operations.

How to prepare the state of the correlation system for a single horizontal line and how to read read it out has already been discussed in Section 1.2.3. Hence the only piece missing for universal quantum computation is a single entangling two-qubit gate.

The schematics for a controlled-Z gate between two horizontal lines in the lattice are given below. We implicitly assume that all adjacent sites not shown are measured in

the Z-basis,

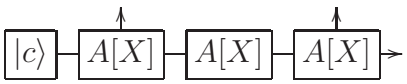


. (1.82)

The measurement scheme realizes a controlled-Z gate, where the correlation system of the lower line carries the control qubit and the upper line the target qubit.

In detail one would proceed as follows: first one performs the X-measurements on the sites shown and the Z-measurements on the adjacent ones. If any of these measurements yields the result "1", we apply a Z-measurement to the central site and restart the procedure three sites to the right. This approach has been chosen for convenience: it allows us to forget about possible phases introduced by other measurement outcomes. Still, the "correct" result will occur after a finite expected number of steps, so the overhead caused due to this simplification is only linear. It is also not hard to see that most other outcomes can be compensated for – so for practical purposes the scheme could be vastly optimized.

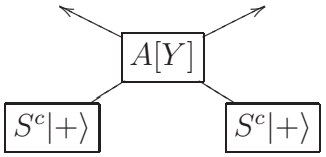
Now assume that all measurements yielded "0". Then a Y-measurement is performed on the central site, obtaining the result y. As we did in Section 1.3.1, we assume that the (lower) control line is in the basis state $|c\rangle$, for $c \in \{0, 1\}$. The contraction of the lower-most three tensors gives



(1.83)

$$= \quad S^c|+\rangle_{lu} S^c|+\rangle_{ru} H|c\rangle_r,$$

where as before $S = S(i) = \mathrm{diag}(1, i)$. We plug this result into the $A[Y]$ tensor:



(1.84)

$$= \quad |+\rangle_{lu}|+\rangle_{ru} + (-1)^{c+y} i(S \otimes S)|+\rangle_{lu}|+\rangle_{ru}.$$

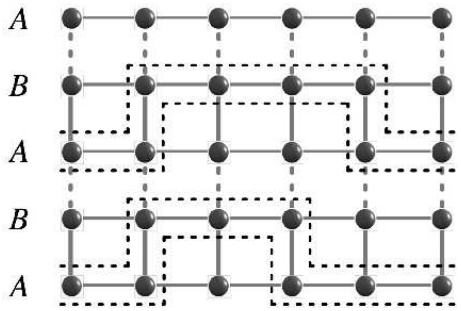
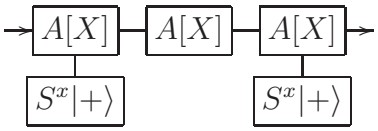


Figure 1.5: Weighted graph state where the gate is achieved by appropriately bringing two wires together in a "rerouting process".

Lastly, for $x \in \{0, 1\}$,



$$= HZ^x. \tag{1.85}$$

Hence, the evolution on the upper line is

$$H(\mathbb{1} + (-1)^{c+y} iZ) \propto HSZ^{y+c}, \tag{1.86}$$

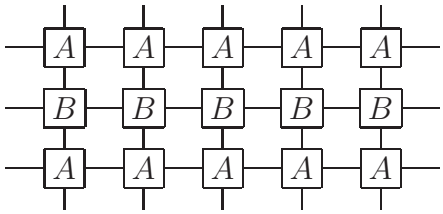
equivalent to Z^c up to by-products. We arrive hence at the following conclusion:

Observation 7 (Non-maximal entangling power)**.** *Universal resouces may be prepared using commuting gates with non-maximal entangling power.*

Rerouting

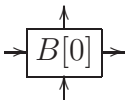
we will consider a second weighted graph state to exemplify yet another novel ingredient that one can make use of in measurement-based quantum computation: One can think of quantum information being transported in the correlation system of some systems on the lattice forming "wires", in a way that gates are realized by bringing the "wires" together. This is an element that is not present in the original one-way computer. The subsequent example of a resource state has not been chosen for its plausibility in the preparation in a physical context, but in a way such that this idea of "rerouting quantum information" can very transparently be explained, see Fig. 1.5.

The resource that we think about is defined by tensors that are fully translationally invariant in one dimension, and has period two in the orthogonal dimension,

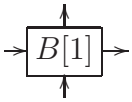


. (1.87)

This is, we have two kinds of tensors: One set is given by



$$= |+\rangle_r |+\rangle_u \langle 0|_l \langle 0|_d, \tag{1.88}$$

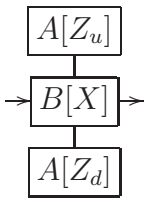


$$= |-\rangle_r |i\rangle_u \langle 1|_l \langle 1|_d \tag{1.89}$$

whereas the other one is nothing but the familiar one for a 2-D cluster state as in Eqs. (1.88, 1.89), with boundary conditions

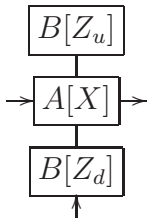
$$|L\rangle = |D\rangle = |+\rangle, \qquad |R\rangle = |U\rangle = |1\rangle. \tag{1.90}$$

The resulting state is hence again a weighted graph state, where in one dimension every second edge is replaced by an edge prepared using a gate with non-maximal entangling power. Then, it is not difficult to see that, again with $x, z_r, z_u, z_d, z_l \in \{0, 1\}$,



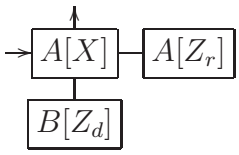
$$= H Z^{x+z_d} S^{z_u}, \tag{1.91}$$

and



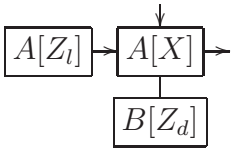
$$= HZ^{x+z_u}S^{z_d}. \tag{1.92}$$

Similarly, we can consider several corner elements in this resource. We obtain

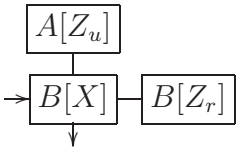


$$= HZ^{x+z_d}S^{z_u}, \tag{1.93}$$

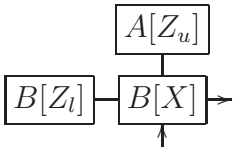
and similarly



$$= (HSH)^{z_d}X^{z_l+x}, \tag{1.94}$$

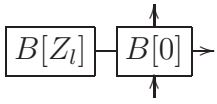


$$= Z^{x+z_r}S^{z_u}, \tag{1.95}$$

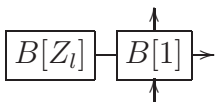


$$= HZ^{x+z_u+z_l}(SZ)^{z_u}, \tag{1.96}$$

where we have again made use of the convention that $x = 0$ corresponds to $|+\rangle$ and $x = 1$ to $|-\rangle$. We need one more ingredient to the scheme, this is

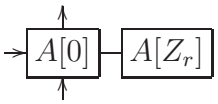


$$= |+\rangle_r|+\rangle_u\langle 0|_d, \tag{1.97}$$

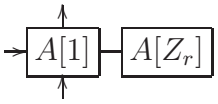


$$= |-\rangle_r|i\rangle_u\langle 1|_d, \tag{1.98}$$

and



$$= |+\rangle_u\langle 0|_l\langle 0|_d, \tag{1.99}$$



$$= (-1)^{z_r}|-\rangle_u\langle 1|_l\langle 1|_d. \tag{1.100}$$

Putting these ingredients, and following an argument similar to the last subsection, we find that up to Clifford group by-products, we can transport along the horizontal lines for both kinds of local tensors. We can also use the corner pieces to reroute as depicted in Fig. 1.5, and bring routes together forming a "gate" imprinted in the lattice, actually, a controlled-S gate.

It should be noted that it is not obviously possible to faithfully transport one qubit of information vertically through the resource. Loosely speaking, the entanglement between a site of type B and the site of type A directly above it is non-maximal (this is indicated by dotted lines in Fig. 1.5). Interestingly, one can still perform a (non-maximally entangling) non-local gate over this connection.

Observation 8 (Rerouting)**.** *Gates in measurement-based quantum computation can be achieved by means of appropriate routing of quantum information in the lattice.*

1.3.4 A qubit resource with non-vanishing correlation functions

We will very briefly sketch a matrix product state on a 1-D chain of qubits, which i) exhibits non-vanishing two-point correlation functions, ii) allows for any unitary to be realized in its correlation system and iii) can be coupled to a universal 2-D resource in a way very similar to the AKLT-type example (Section 1.3.1). The discussion will be somewhat superficial – however, given the extensive discussion of other models above, the reader should have no problems filling in the details.

Choose an integer $m > 2$ and define

$$G := \exp(i\pi/mX). \tag{1.101}$$

Up to a constant, G is a m-th root of X. The state is defined by the following relations:

$$\rightarrow\boxed{A[s]}\rightarrow \quad = \quad |s\rangle_r\langle s|_l G, \tag{1.102}$$

and

$$|L\rangle = G^\dagger|+\rangle, \quad |R\rangle = |+\rangle. \tag{1.103}$$

The two-point correlation functions for measurements on this state never vanish completely. Indeed, in Appendix 1.6.1 it will be shown that

$$\langle Z_i Z_{i+k}\rangle - \langle Z_i\rangle \langle Z_{i+k}\rangle = 2\xi^k, \tag{1.104}$$

where $\xi := 2\sin^2(\pi/m) - 1$.

For X-measurements, we find

$$\rightarrow\boxed{A[X]}\rightarrow \quad = \quad Z^x G \tag{1.105}$$

Pursuing the strategy introduced in Section 1.3.1, we set the by-product group to $\mathcal{B} = \langle Z, G\rangle$, so the group generated by Z and G. One can easily verify that $\mathcal{B}$ is indeed a finite group, equivalent to the *dihedral group* of order $2m$.

It is now straight-forward to check that i) measurements in the computational basis can be used for preparation and read-out (as in Section 1.2.3), ii) general local unitaries can be realized by means of measurements in the equatorial plane of the Bloch sphere (as in Section 1.3.1) and iii) a 2-D resource is obtainable in a fashion similar to the one presented in Section 1.3.1. With similar methods, one can also find qubit resource states that have a local entropy smaller than unity.

1.3.5 Percolation ideas to make use of imperfect resources

For completeness, we mention yet another kind of resource: This is an imperfect cluster state where some edges are missing. Such a setting is clearly relevant in a number of physical situations: If the underlying quantum gates building up the cluster state are fundamentally probabilistic, such as in linear optical architectures, then one very naturally arrives at this situation when one aims at minimizing the need for feed-forward. A

similar situation is encountered in cold atoms in optical lattices, when in a Mott state exhibiting hole defects some atoms are missing. We do not present details of such arguments, which have been considered in Ref. [68], based on ideas of *edge percolation* and renormalization [44]. We merely state the result for completeness. Note also that results that may be similar to these ones have been announced in Ref. [109].

We consider the setting where one starts from a 2-D or 3-D cubic lattice of size $n \times n$. Two neighboring vertices on the lattice are connected with an edge with probability p. The stochastic variables deciding whether or not an edge is present are assumed to be uncorrelated. If $p > p_2 = 1/2$ holds, then it is not difficult to see that one can extract a 2-D renormalized lattice of smaller size: This means that one can find a function $n \mapsto m(n)$, such that one arrives at a cubic $m(n) \times m(n)$ array almost certainly as $n \to \infty$, with the following property: Within each of the elements of this array, there is a central site that is connected to the central site of the neighboring array. Since all the additional sites can be removed by means of Z-measurements, we can treat this resource effectively as a 2-D cluster state of dimension $m(n) \times m(n)$, and refer to this as a *perfect sublattice*. This state will not necessarily be exactly a cluster state, as it may contain vertices having a vertex degree of three, but which will nevertheless function as a graph state resource just as the cluster state does (for details, see Ref. [68]). Also, $n/m(n)$ is arbitrarily close to being linear in n asymptotically. However, an even stronger statement holds:

Observation 9 (Percolation)**.** *Whenever $p > p_3 = 0.249$, for any $\varepsilon > 0$, one can find a function $n \mapsto m(n)$ with the following property: Starting from a sublattice of a 3-D cubic lattice of size $n \times n \times 2n/m(n)$, one can almost certainly prepare a perfect sublattice of size $m(n) \times m(n)$. The asymptotic behavior of m can be chosen to satisfy*

$$n/m(n) = O(n^{\varepsilon}). \tag{1.106}$$

That is, with an overhead that is arbitrarily close to the optimal scaling, one can obtain a perfect resource state out of an imperfect one, even if one is merely above the percolation threshold for a three-dimensional lattice, and not only for the two-dimensional lattice, see Fig. 1.6. The latter argument is technically more involved than the former, for details, see Ref. [68]. This shows, however, with methods unrelated to the ones con-

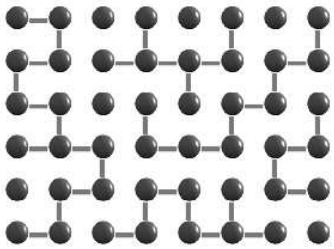


Figure 1.6: Cubic lattice of a graph state corresponding to the situation where some edges are missing in a cluster state. If the probability p of having an edge is sufficiently high the processes independent, then a renormalized perfect sublattice can be found almost certainly, giving rise to a cluster state of smaller size. If $p > p_2 = 1/2$, where p_2 is the percolation threshold for edge percolation in 2-D cubic lattices, then a renormalized lattice can be found almost certainly. Interestingly, even if $1/2 > p > p_3$, $p_3 = 0.249$ denoting the percolation threshold in 3-D, one can almost certainly construct a perfect sublattice, using an overhead that is arbitrarily close to being quadratic.

sidered primarily in the present work, that also random aspects in the resource as such can be dealt with.

1.4 One-way computation using encoded systems

In the final section of this work, we will show that one can find resource states for MBQC that differ substantially from the cluster in various entanglement properties. This will be done by encoding each system of a resource into several physical particles. We will not develop any new computational models and make no use of the computational tensor network formalism introduced before. The study of encoded resource states was initiated in Ref. [6] and later pursued more systematically in Ref. [107].

More concretely, the following statements will be proved:

Observation 10 (Resources with weak capabilities for state preparation)**.** *There exists a family of universal resource states such that*

- *The local entropy of entanglement is arbitrarily small,*
- *The localizable entanglement is arbitrarily small*

and, more strongly,

- *The probability of succeeding in distilling a maximally entangled pair out of the resource is arbitrarily small, even if one does not a priori fix the two sites between which the pair will be established.*

In particular, the resource cannot be used as a state preparator.

We start from a cluster state vector on $n \times n$ systems, denoted by $|Cl_{n\times n}\rangle$, referred to as logical qubits. As in Ref. [6], we want to "dilute" the cluster state, i.e. encode it into a larger system, by means of invoking the codewords

$$|\tilde{0}\rangle := |0\rangle^{\otimes k},\ |\tilde{1}\rangle := |W_k\rangle \tag{1.107}$$

for some parameter k. The argument relies only on the choice of $|W_k\rangle$ as a code word in that we focus on its implications on the localizable entanglement, and for that argument, the state vector $|W_k\rangle$ has the desired properties of small local entropy and permutation invariance. However, for encoded one-way computation to be possible, any state vector orthogonal to $|0\rangle^{\otimes k}$ may be taken, compare also Ref. [107]. Every qubit of the cluster is subjected to the encoding operation

$$V := |\tilde{0}\rangle\langle 0| + |\tilde{1}\rangle\langle 1| \tag{1.108}$$

yielding the *diluted cluster* $|\mathcal{D}_{n,k}\rangle$. A set of physical qubits corresponding to one cluster bit will be called a *block*. As before, by a *local measurement scheme* we mean a sequence of adaptive local projective measurements, local to the physical systems.

Let us first show again in more detail that such an encoding constitutes no obstacle to universal quantum computation. Each of the code words is orthogonal, and for computation to be possible, we need to do local dichotomic measurements in the logical space. By Ref. [118], any two pure orthogonal multi-partite states on k qubits can be deterministically distinguished using LOCC. By making use of the construction of Ref. [118], this can be done by an appropriate ordered sequence of adapted projective measurements $\pi_1 \otimes \cdots \otimes \pi_k$ on the sites of each codeword, giving rise to an arbitrary projective dichotomic measurement with Kraus operators

$$A_1 := |\psi\rangle\langle\psi|,\ A_2 := |\psi^\perp\rangle\langle\psi^\perp| = \mathbb{1} - |\psi\rangle\langle\psi| \tag{1.109}$$

in the logical space, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ and $|\psi^{\perp}\rangle = -\beta^*|0\rangle + \alpha^*|1\rangle$. Hence, one can translate any single-site measurement on a cluster state into an LOCC protocol for the encoded cluster. This shows that $|\Psi\rangle$ is universal for deterministic MBC. This is the argument of Ref. [6] (see also Ref. [107] for a more detailed and extensive discussion on one-way computing based on encoded systems).

In the following we are going to show in more detail that despite this property, we are heavily restricted to use this resource to prepare states with a significant amount of entanglement between two constituents. In fact, we can not even distill a perfect maximally entangled qubit pair beyond any given probability of success. This means that these states are universal resources, but on the level of physical systems utterly useless for state preparation. The given resource is, needless to say, not meant as a particularly feasible resource. Instead, we aim at highlighting to what extent as such the entanglement properties can be relaxed, giving a guideline to more general settings.

Note first that the localizable entanglement E_L in these resources can easily be shown to be arbitrarily small: The entropy for a measurement in the computational basis reads $H_b(3/(4k+2))$, where $H_b : [0,1] \to [0,1]$ is the standard binary entropy function. Using the concavity of the entropy function, we find

$$E_L(|\mathcal{D}_{n,k}\rangle\langle\mathcal{D}_{n,k}|) \leq H_b(3/(4k+2)), \tag{1.110}$$

such that $\lim_{k\to\infty} E_L(|\mathcal{D}_{n,k}\rangle\langle\mathcal{D}_{n,k}|) = 0$. This means that for two fixed sites, the rate at which one can distill maximally entangled pairs by performing measurements on the remaining systems is arbitrarily small.

This can be seen as follows. We will aim at preparing a maximally entangled state between any two constituents of two different blocks. It is easy to see that within the same block, the probability of success can be made arbitrarily small. We hence look at a LOCC distillation scheme, a *measurement-based scheme*, taking the input ρ and producing outputs

$$\rho \mapsto K_j \rho K_j^{\dagger} \tag{1.111}$$

with probability $p_j = \mathrm{tr}(K_j \rho K_j^{\dagger})$, $j = 1, \ldots, J$. This corresponds to a LOCC procedure, where each of the measurements may depend on all outcomes of the previous

local measurements. Let us assume that outcomes labeled $1, \ldots, S$ for some $S \leq J$ are successful in distilling a maximally entangled state.

We start by exploiting the permutation symmetry of the code words. Choose a block i of $|\mathcal{D}_{n,k}\rangle$. Assume there exists a measurement-based scheme with the property that with probability p, the scheme will leave *at least one* system of block i in a state of maximal local entropy. Then there exists a scheme such that with probability p, the scheme will leave *the first* system of block i in a state of maximal local entropy. At some point of time the scheme is going to perform the first measurement on the i-th block. Because of permutation invariance, we may assume that it does so on the k-th system of the block. The remaining state is still invariant under permutations of the first $k-1$ systems. Hence there is no loss of generality in assuming that the next measurement on the i-th block will be performed on the $k-1$-st system. If the local entropy of any of the unmeasured systems is now maximal, then the same will be true for the first one – once again, by permutation invariance.

Also, it is easy to see that the probability p that a measurement-based scheme will leave any system of block i in a locally maximally mixed state is bounded from above by

$$p < 2/k. \tag{1.112}$$

Let p_1 be the initial probability of obtaining the outcome $|1\rangle$ for a Z measurement on this qubit, $p_1 = |\langle 1|\mathcal{D}_{n,k}\rangle|^2$. Clearly,

$$p_1 < 1/k. \tag{1.113}$$

We consider now a local scheme potentially acting on all qubits except this distinguished one, with branches labeled $j = 1, ..., J$, aiming at preparing this qubit in a maximally mixed state. Let p_s be the probability of the qubit ending up in a locally maximally mixed state. In case of success, so in case of the preparation of a locally maximally entangled state, we have that $p_1(s) = 1/2$, in case of failure $p_1(f) \geq 0$. Combining these inequalities, we get

$$1/k > p_1 = p_s p_1(s) + (1 - p_s)p_1(f) = p_s/2. \tag{1.114}$$

We can hence show that there exists a family of universal resource states such that the probability that a local measurement scheme can prepare a maximally entangled qubit pair (up to l.u. equivalence) out of any element of that family is strictly smaller than $\varepsilon > 0$.

Let p_i be the probability that a site of block i will end up as a part of a maximally entangled pair. This means that when we fix the procedure, and label as before all sequences of measurement outcomes with $j = 1, ..., J$, one does not perform measurements on all constituents. Let I denote the index set labeling the cases where somewhere on the lattice a maximally entangled pair appears, so the probability p for this to happen is bounded from above by

$$p \leq \sum_{i \in I} p_i. \tag{1.115}$$

According to the above bound, $p_i < 2/k$, giving a strict upper bound of $p \leq 2n^2/k$ for the overall probability of success. The family

$$|\Psi_n\rangle := |\mathcal{D}_{n,k(n)}\rangle, \tag{1.116}$$

for $k(n) := 2\varepsilon^{-1}n^2$ is clearly universal, involves only a linear overhead as compared to the original cluster state and satisfies the assumptions advertised above.

1.5 Conclusions

In this work, we have shown how to construct a plethora of novel models for measurement-based quantum computation. Our methods were taken from many-body theory. The new models for quantum computation follow the paradigm of locally measuring single sites – and hence abandoning any need for unitary control during the computation. Other than that, however, they can be quite different from the one-way model. We have found models where the randomness is compensated in a novel manner, the length of the computation can be random, gates are performed by routing flows of quantum information towards one another, and logical information may be encoded in many correlation systems at the same time. What is more, the resource states can in fact be radically different from the cluster states, in that they may display correlations as typi-

cal in ground states, can be weakly entangled. A number of properties of resource states that we found reasonable to assume to be necessary for a state to form a universal resource could be eventually relaxed. So after all, it seems that much less is needed for measurement-based quantum computation than one could reasonably have anticipated. This new degree of flexibility may well pave the way towards tailoring computational model towards many-body states that are particularly feasible to prepare, rather than trying to experimentally realize a specific model.

1.6 Appendix

1.6.1 Computing correlations functions

What is the value of the two-point correlation function $\langle Z_i Z_{i+k}\rangle - \langle Z_i\rangle \langle Z_{i+k}\rangle$? In this work, we have only introduced the behavior of the correlation system when subject to a local measurement of a rank-one observable. However, in order to evaluate the correlation function, we need "measure the identity" on the intermediate systems or, equivalently, trace them out. Without going into the general theory [35], we just state that tracing out a system will cause the completely positive map

$$\Phi : \rho \mapsto \sum_i A[i]\rho A[i]^\dagger \tag{1.117}$$

to act on the correlation system.

For the cluster state, using the fact that the bases $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ are unbiased, we can easily show that Φ^2 is the completely depolarizing channel, sending any ρ to $2^{-1}\mathbb{1}$. This causes any correlation function to vanish for $k > 2$. How does the situation look like for the state vector defined by Eq. (1.102)? We compute:

$$\Phi : \rho \mapsto \sum_{s=0,1} \mathrm{tr}(\rho\, G|s\rangle\langle s|G^\dagger)\, |0\rangle\langle 0|, \tag{1.118}$$

so for $s \in \{0, 1\}$:

$$\Phi(|s\rangle\langle s|) = p|s\rangle\langle s| + (1-p)|\bar{s}\rangle\langle\bar{s}| \tag{1.119}$$

where $\bar{0} := 1, \bar{1} := 0$ and $p := |\langle 0|G|0\rangle|^2 = \sin^2(\pi/m)$. In other words: when acting on the computational basis, Φ implements a simple two-state Markov process, which remains in the same state with probability p and switches its state with probability $(1-p)$. Now, $\langle Z_i Z_{i+k}\rangle$ equals $+2$ if an even number of state changes occurred and -2 if that number is odd. So for the expectation value we find

$$\begin{aligned}\langle Z_i Z_{i+k}\rangle &= 2\sum_{l=0}^{k+1}\binom{k}{l}p^{k-l}(1-p)^k(-1)^k \\ &= 2(2p-1)^k = 2(2\sin^2(\pi/m)-1)^k.\end{aligned} \tag{1.120}$$

1.6.2 Hamiltonian of the AKLT-type state

In Section 1.3.1 we discussed an AKLT-type matrix product state. It was claimed that the state constitutes the unique ground-state of a spin-1 nearest neighbor frustration free gapped Hamiltonian. It must be noted that in this work, we have not introduced the technical tools needed to cope with boundary effects at the end of the chain. There are at least three ways to make the above statement rigorous: a) treat the statement as being valid asymptotically in the limit of large chains, b) work directly with infinite-volume states [35], or c) look at sufficiently large rings with periodic boundary conditions [84]. Once one chooses one of the options outlined above, the proof of this fact proceeds along the same lines as the one of the original AKLT state, as presented in Example 7 of Ref. [35] (see also Ref. [84]). Indeed, using the notions of Refs. [35, 84] one verifies that

$$\Gamma_2 : \mathcal{B}(\mathbb{C}^2) \to \mathbb{C}^2 \otimes \mathbb{C}^2, \tag{1.121}$$

$$B \mapsto \textstyle\sum_{i_1,i_2=1}^{3} \mathrm{tr}(BA[i_1]A[i_2])|i_1, i_2\rangle \tag{1.122}$$

is injective. Further, if $\mathcal{G}_2 := \mathrm{range}\,\Gamma_2$, it is checked by direct computation that $\dim(\mathcal{G}_2 \otimes \mathbb{1} \cap \mathbb{1} \otimes \mathcal{G}_2) = \dim \mathcal{G}_2$. All claims follow as detailed in Refs. [35, 84].

In particular, let h be a positive operator supported on the vector space spanned by:

$$\begin{aligned}&\{|1,1\rangle, |2,2\rangle, -(1/4)|0,0\rangle + |1,2\rangle + |2,1\rangle, \\ &-(1/\sqrt{8})|0,0\rangle + |0,2\rangle + |2,0\rangle, \\ &-(1/\sqrt{8})|0,0\rangle + |0,1\rangle + |1,0\rangle\}.\end{aligned} \tag{1.123}$$

Set $H := \sum_i \tau_i(h)$, where τ_i translates its argument i sites along the chain. Then H is a non-degenerate, gapped, frustration free, nearest neighbor Hamiltonian (called *parent Hamiltonian* in Ref. [84]), whose energy is minimized by the state at hand.

2

Computational quantum wires as primitives in measurement-based schemes

2.1 Introduction

In this chapter, we aim to give a complete classification of a natural primitive of measurement-based computation. Our approach is best motivated by considering the cluster state. The state comes in two versions, defined on a one-dimensional or on a two-dimensional lattice respectively. In order to prove universality of the cluster, it is expedient to first understand how one-dimensional states can be used to transport and process one logical qubit. Then, in a second step, one proves that these one-dimensional "computational wires" can be coupled in a suitable fashion, to form a fully universal 2-D resource.

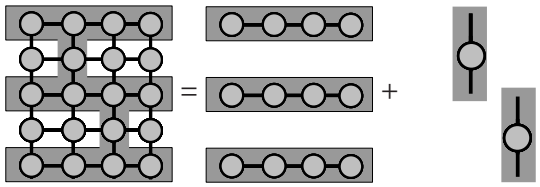


Figure 2.1: In this chapter, we are concerned with universal resource states which can be decomposed states into horizontal chains of quantum systems (representing logical qubits) and couplings between these chains (mediating non-local logical interactions).

We will turn this convenient property into an axiom. All states considered below can be prepared in a two-step process (see Fig. 2.1). First, one entangles horizontal lines of physical systems. Each of these lines will represent a logical qubit during the measurement-based calculation. We are interested in states of these chains which are "universal". Roughly, this means that by means of local measurements alone, one should be able to transport and process one qubit worth of quantum information. This concept – which is somewhat stronger than demanding the lines have maximal localizable entanglement [88] – will be made more precise below.

We will refer to such states on a 1-D chain of quantum systems as *computational quantum wires*. At this step, we actually aim for complete generality: we will characterize all qubit computational wires which can be built up by nearest-neighbor entangling operations.

In a second step, it will be shown how to couple several wires together, in order to form a truly universal state on a 2-D lattice. The coupling will be facilitated by a

controlled-phase type operation.

For simplicity, this paper focuses on qubits and translationally invariant states. Neither requirement is, however, crucial for the techniques detailed below.

2.1.1 Technical setup

The main mathematical tool used in this chapter are matrix product states (MPS), as introduced in detail in Chapter 1. Some further technical details are discussed in Section 2.4.2.

All states we will be concerned with are of the form

$$|\Psi_n\rangle = \sum_{x_1,\ldots,x_n=0}^{1} \langle R|A[x_n]\ldots A[x_1]|L\rangle \; |x_1,\ldots,x_n\rangle. \tag{2.1}$$

for two 2×2-matrices $A[0/1]$ and appropriate boundary conditions $|L\rangle, |R\rangle$.

We recall the basic tenet of Chapter 1. To that end, let

$$|\phi_1\rangle \otimes \cdots \otimes |\phi_n\rangle$$

be a product vector. Set

$$A[\phi_i] = \langle \phi_i|0\rangle \, A[0] + \langle \phi_i|1\rangle \, A[1]. \tag{2.2}$$

It is elementary to verify that

$$(\langle \phi_1| \otimes \ldots \langle \phi_n|)|\Psi\rangle = \langle R|A[\phi_n]\ldots A[\phi_1]|L\rangle. \tag{2.3}$$

One can hence explicitly compute the overlap of $|\Psi_n\rangle$ with any local projection operator and therefore the probability of obtaining the associated outcome when performing local projective measurements. Now, if one performs a projective measurement on the ith site and obtains a measurement outcome corresponding to ϕ_i, then one causes the operator $A[\phi_i]$ to act on the correlation space in Eq. (2.3). Depending on the state and on the measurement basis, this operator might be unitary. Hence, a local measurement on an MPS may be understood as giving rise to a "formal single-qubit computation in the

correlation space". As detailed Chapter 1, this formal intuition can be made precise: *measurement-based computation takes place in correlation space*.

So in order to evaluate the computational usefulness of a given state $|\Psi_n\rangle$, one should derive its MPS representation and then check which unitary operations can be realized in correlation space by means of appropriate local measurements. This is the programme carried out below.

2.2 Computational quantum wires

By a *computational wire* we mean a family of pure states $|\Psi_n\rangle$, where

(i) $|\Psi_n\rangle$ is defined on a 1-D chain of n qubits,

(ii) $|\Psi_n\rangle$ is preparable from the product state

$$|\mathbf{0}_n\rangle = |0\rangle \otimes \cdots \otimes |0\rangle \in (\mathbb{C}^2)^{\otimes n}$$

by the sequential action of a nearest-neighbor unitary gate U:

$$|\Psi_n\rangle = U^{(n,n-1)} \ldots U^{(3,2)}\, U^{(2,1)}\, |\mathbf{0}_n\rangle, \tag{2.4}$$

(iii) in the limit of large n, the entropy of entanglement between the left half and the right half of the chain approaches one ebit.

These axioms may seem surprisingly weak. Indeed, in the introduction, we loosely characterized computational wires as states with the power to "transport and process one logical qubit by means of local measurements". It is one central result of this work that any state fulfilling *(i)* – *(iii)* is automatically useful for information processing, as made precise below.

Note that the 1-D cluster states $|Cl_n\rangle$ are computational wires. In this case, the entangling nearest-neighbor unitary U is given by the controlled-Z gate.

2.2.1 Summary of results

The following main results are obtained in this chapter.

- Discounting local basis changes, there is a three-parameter family of computational wires, which can be explicitly parameterized.
- For any wire, there is a one-parameter set of measurement bases, such that the operation implemented on correlation space is unitary, irrespective of the measurement outcome.
- Except for a set of measure zero, all computational wires allow for the implementation of any unitary transformation $\in SU(2)$ in its correlation space.
- A quantum wire may be specified by *(i)* an "always-on operation" $W \in SU(2)$, which acts on the correlation space after any step, independent of the basis chosen or measurement outcome obtained, and *(ii)* a "by-product angle" ϕ, specifying how sensitive the resource is to the inherent randomness of quantum measurements.
- There are "universal" computational wires, which are locally arbitrarily close to a pure state. Previously explored resources with low local entanglement were obtained by using non-local encodings (see Chapter 1) of maximally entangled resource states. In the case of the states considered here, the effect is inherent.
- One-dimensional computational wires may be easily coupled using controlled-Z type entangling operations. Non-local gates between the logical qubits carried in each 1-D strand can be implemented by means of local measurements.

2.2.2 Characterization of all computational wires

The first step is to realize that any computational wire automatically has a simple MPS representation with bond dimension two. This is a convenient state of affairs: in the previous chapter, we had to restrict generality by focusing on states with simple MPS representations – here, this feature emerges naturally.

Lemma 11. *If a state $|\Psi_n\rangle$ fulfills points (i), (ii) above, then it has an MPS representa-*

tion

$$|\Psi_n\rangle \tag{2.5}$$
$$= \sum_{x_1,\ldots,x_n=0,1} \left(\langle 0|B[x_n]A[x_{n-1}]\ldots A[x_1]|0\rangle\right)|x_1,\ldots,x_n\rangle,$$

where $A[0], A[1]$ *are* 2×2*-matrices and* $B[x] = |0\rangle\langle x|$.

Note that the nth qubit plays a special role in Eq. (2.5), thus breaking the translational invariance of the MPS representation found in Eq. (2.1). Physically, it is clear that the final qubit is distinguished: it is the only site which does not occur as the input of U in Eq. (2.4). Fortunately, this inhomogeneity turns out to be irrelevant for our computational scheme.[1] We will hence ignore it in what follows.

Proof. Set ${U^{(i,j)}}_{(k,l)} = \langle i,j|U|k,l\rangle$ and define

$${A[x]^i}_j = {U^{(x,i)}}_{(j,0)}.$$

Then, using Eq. (2.4) and implying summation over repeated indices,

$$\begin{aligned}
& \langle x_1,\ldots,x_n|\Psi_n\rangle \\
= \;& {U^{(x_n,x_{n-1})}}_{(0,y_{n-1})}\ldots {U^{(x_2,y_2)}}_{(0,y_1)}\,{U^{(x_1,y_1)}}_{(0,0)} \\
= \;& {A[x_{n-1}]^{x_n}}_{y_{n-1}}\ldots {A[x_2]^{y_2}}_{y_1}{A[x_1]^{y_1}}_0 \\
= \;& \langle 0|(|0\rangle\langle x_n|)A[x_{n-1}]\ldots A[x_1]|0\rangle \\
= \;& \langle 0|B[x_n]A[x_{n-1}]\ldots A[x_1]|0\rangle,
\end{aligned}$$

proving the claim. □

As indicated before, local measurements in a basis $\{|\phi\rangle, |\phi^\perp\rangle\}$ can directly be interpreted as a quantum computation in correlation space if the associated operators $A[\phi], A[\phi^\perp]$ are unitary (up to normalization). For a general MPS, such a local basis need not exist. For computational wires, however, this is always true as shown in the

[1] To make that claim manifest, one could measure out the nth qubit in the computational basis. Denote the result of the measurement by $x \in \{0,1\}$. The resulting state on sites $1,\ldots,n-1$ has the homogeneous form of Eq. (2.1), where $\langle R| = \langle 0|B[x]$.

next Lemma. This finding is a precise statement of the earlier claim that wires are good for the "transport of one logical qubit" in correlation space.

Lemma 12. *Let $|\Psi_n\rangle$ be a computational wire. Then – after a suitable local basis change – it admits an MPS representation as in Eq. (2.5), where*

$$\begin{aligned} A[0] &= \sin\gamma\, U_0, \\ A[1] &= \cos\gamma\, U_1 \end{aligned} \tag{2.6}$$

for some real γ and unitaries $U_i \in U(2)$.

Proof. Let $A[0], A[1]$ be the matrices defining the MPS representation of $|\Psi_n\rangle$ as in Lemma 11. By Section 2.4.2, Lemma 23 and Lemma 27, the channel

$$\hat{\mathbb{E}} : \rho \mapsto A[0]\rho A[0]^\dagger + A[1]\rho A[1]^\dagger$$

has Kraus operators $A'[0/1]$ of the form given in Eq. (2.6). There exists a unitary matrix V relating the two sets of Kraus operators:

$$\begin{aligned} \sin\gamma U_0 &= A'[0] = V^0{}_0\, A[0] + V^0{}_1\, A[1] \\ \cos\gamma U_1 &= A'[1] = V^1{}_0\, A[0] + V^1{}_1\, A[1]. \end{aligned}$$

By Eqs. (2.2,2.3),

$$A'[0] = A[V|0\rangle], \qquad A'[1] = A[V|1\rangle]$$

so that the primed matrices give the MPS representation of $|\Psi_n\rangle$ in the basis $\{V|0\rangle, V|1\rangle\}$. □

The MPS representation of a state vector is not unique. In the following, we use various degrees of gauge freedom to identify the relevant set of parameters defining computational wires.

We will make repeated use of the *ϕ-phase gate*

$$S(\phi) = \mathrm{diag}(e^{-i\phi/2}, e^{i\phi/2}) \in SU(2).$$

Theorem 13. *A computational wire is described by*

- *an "always-on evolution" $W \in SU(2)$ and*
- *a "by-product rotation angle" $\phi \in \mathbb{R}$*

in the sense that it allows for an MPS representation where

$$\begin{aligned} A[0] &= 2^{-1/2}\, W, \\ A[1] &= 2^{-1/2}\, W\, S(\phi). \end{aligned} \tag{2.7}$$

What is more, there is no loss of generality in assuming that W is of the form

$$W = e^{i \sin\alpha/2 (\sin\beta X + \cos\beta Z)} \in SU(2).$$

for suitable $\alpha, \beta \in \mathbb{R}$.

Proof. A matrix product state does not change when we conjugate both defining matrices with the same unitary. With this realization in mind, and arguing as in Lemma 12, the result follows from Lemma 25. □

Equation (2.7) goes a long way towards understanding the structure of computational wires. Assume that we measure site by site in the computational basis. Then at every step the operation W will be applied to the correlation system, irrespective of the measurement outcome. We will refer to W as the *always-on operation*. However, some tribute must be paid to the random nature of quantum measurements. This comes in the form of the *by-product* operation $S(\phi)$, which acts on the correlation system in case the "wrong" measurement outcome ("1", instead of "0") is obtained. It is remarkable that this penalty is fully described by a single parameter: the *by-product angle* ϕ.

The cluster state serves as the paradigmatic example. Here, the always-on operation is $W = H$, the Hadamard gate. The by-product angle is π, so that a "wrong" measurement outcome will cause an extra $S(\pi) \propto Z$ operation to be applied. Note that H is already in the form given in Eq. (2.29); with $\alpha = \pi$ and $\beta = \pi/4$.

It turns out that there is a second normal form for computational wires, which is equally insightful. Indeed, we have:

Theorem 14. *A computational wire is described by*

- *an "always-on evolution" $W' \in SU(2)$ and*
- *a "bias parameter" $\gamma \in \mathbb{R}$*

in the sense that it allows for an MPS representation where

$$\begin{aligned} A[0] &= \sin\gamma\, W', \\ A[1] &= \cos\gamma\, W'\, S(\pi). \end{aligned} \tag{2.8}$$

What is more, there is no loss of generality in assuming that W' is of the form

$$W' = e^{i \sin\alpha/2(\sin\beta X + \cos\beta Z)} \in SU(2).$$

for suitable $\alpha, \beta \in \mathbb{R}$.

Proof. As in Theorem 13, employing Lemma 24. □

The relationship between the by-product angle and the bias angle characteristic of the two normal forms above is simply $\phi = 4\gamma$, as will be shown in Lemma 21.

From Theorem 14 we conclude that by measuring in an appropriate basis, we may always assume that the by-product operator is $S(\pi) \propto Z$, as is the case for the cluster state. However, the probability of obtaining the one outcome or the other is no longer $1/2$, but given by $\sin^2\gamma$ and $\cos^2\gamma$ respectively (see also Sec. 2.2.4). This is a remarkable fact: when using a computational wire to process unknown quantum states by local measurements, we must take care not to learn any information about the correlation system, as this would obviously destroy the coherence of the process. For the cluster state, it is manifestly true that no information is obtained, as the local measurements yield completely random outcomes. The theory of more general computational wires shows that "oblivious quantum information processing" by local measurements is not tied to completely random outcomes.

Also, it becomes clear that in general computational wires, the local sites are not maximally entangled with respect to the rest of the lattice. This phenomenon will be explored quantitatively in Section 2.2.6.

From now on, we will always assume that computational wires are in the "$\phi - W$-normal form" introduced in Theorem 13.

It remains to prove the converse of Theorem 13. Is it the case that there exists a legitimate computational wire for every choice of W, ϕ? In principle, the answer is "yes". There is one subtlety, however. As explained in Section 2.4.2, a matrix product state is (asymptotically[2]) completely specified by the defining matrices $A[0/1]$ independently of the boundary conditions only if the channel

$$\hat{\mathbb{E}} : \rho \mapsto A[0]\rho A[0]^\dagger + A[1]\rho A[1]^\dagger$$

has a spectral gap. By Lemma 27, $\hat{\mathbb{E}}$ fails to have a spectral gap if and only if either W' is diagonal or $W' = X$. In order to avoid technical difficulties, we will often exclude this case from our analysis by invoking the following assumption.

Assumption 15. *Assume that $\hat{\mathbb{E}}$ has a spectral gap. Equivalently, assume that W' is neither diagonal nor equal to X.*

Interestingly, it turns out that the wires excluded by this assumption would anyway not allow us to implement arbitrary $SU(2)$-rotations on correlation space as shown in Section 2.2.4. Hence, no relevant cases are lost.

Lemma 16. *Let $|\Psi_n\rangle$ be an MPS of the form given in Eqs. (2.5,2.6). Under Assumption 15, it holds that $|\Psi_n\rangle$ is a computational wire.*

Proof. We have to verify properties *(ii)* and *(iii)*.

To construct a preparation procedure for the state, we reverse the first step of the proof of Lemma 11 and define

$$U^{(x,i)}{}_{j,0} = A[x]^i{}_j.$$

This set of numbers can be completed to a unitary matrix if and only if the jth column $U^{(x,i)}{}_{j,0}$ with elements labeled by x, i form an orthonormal system. But this can easily

[2]Many properties of computational quantum wires can easily be calculated explicitly in the limit of long chains, when the boundary conditions cease to play any role. Fortunately, their influence is suppressed *exponentially* in the distance from the boundary (see Section 2.4.2), so that the "asymptotic" behavior becomes relevant even for relatively small chains.

be checked:

$$\begin{aligned}\sum_{x,i} U^{(x,i)}{}_{j,0}\bar{U}^{(x,i)}_{j',0} &= \sum_i \left(A[0]^i{}_j\bar{A}[0]^i{}_{j'} + A[1]^i{}_j\bar{A}[1]^i{}_{j'}\right)\\ &= \delta_{j,j'}\sin^2\beta + \delta_{j,j'}\cos^2\beta\\ &= \delta_{j,j'},\end{aligned}$$

having made use of the assumption that $A[0/1]$ are proportional to unitaries.

The map $\hat{\mathbb{E}}$ is clearly unital and it is gapped by assumption. So the fact that the entropy of entanglement becomes maximal in the limit of large n is just the content of Proposition 28. □

2.2.3 Examples

Cluster state

The paradigmatic example of a computational wire is the cluster state. Note that in the original definition of the cluster, one has to measure local sites in the X-eigenbasis in order to transport information along the chain, whereas we have chosen to use the computational basis for that purpose. Obviously, the two definitions differ only by the local transformation $H^{\otimes n}$. It has already been mentioned that the parameters of the cluster state

$$W = H, \qquad \phi = \pi.$$

The by-product angle π is the highest possible value.

The T-resource

The $\pi/2$-phase gate $S(\pi/2)$ is sometimes denoted by T. It is of interest partly because T and H generate a finite group: the 12-element single-qubit Clifford group. This fact will help us to compensate the randomness of measurement outcomes, as detailed in Section 2.2.7. We will refer to the computational wire with parameters

$$W = H, \qquad \phi = \pi/2$$

as the T-*resource*, the name referring to its by-product operator.

Superficially, the T-resource seems very close to the cluster state, differing from the well-known state only in the by-product angle. However, there is an important physical difference: the entropy of entanglement of a single site with respect to the rest of the chain is not maximal! (Note that this does not contradict property *(iii)* of the definition of a computational wire). We will prove this fact in Section 2.2.6, where the entanglement of a single site as a function of ϕ is made explicit. In any case, the fact has a simple intuitive explanation. Note that unlike $S(\pi) \propto Z$, the gate $S(\pi/2) = T$ does not have the power to orthogonalize an input vector:

$$|\langle\psi|T|\psi\rangle| > 0, \qquad \forall\, |\psi\rangle.$$

Now consider a measurement of a given site in the computational basis. Because the by-product operator T is "close" to the identity, the state of the correlation system after the measurement depends only "weakly" on the outcome. Hence any given site has only "little power" to change the state on the remainder of the lattice. In other words: the entanglement is low.

It is perhaps remarkable that universal transformations may be realized in the correlation space of such a computational wire, even though any single measurement only has a weak impact (this will be proved in Section 2.2.4).

Correlations

The following wire has been introduced in Chapter 1 to show that universal quantum computation is possible even when the two-point correlators

$$\langle Z_i\rangle \langle Z_{i+k}\rangle - \langle Z_i \otimes Z_{i+k}\rangle$$

between distant sites never vanish. The parameters are

$$W = e^{i\pi/mX}, \qquad \phi = \pi.$$

The absolute value of the correlation function above is given by $(\cos\frac{\pi}{m})^k$ (c.f. Chapter 1).

2.2.4 Operations on correlation space

In order to *process* information in the correlation space – rather than just *transporting* it – we need some freedom to choose which operation to apply. Let

$$|\alpha(\theta,\epsilon)\rangle = \sin\theta|0\rangle + e^{i\epsilon}\cos\theta|1\rangle$$

be a general state vector and consider the associated correlation space operation

$$\begin{aligned} A[\alpha(\theta,\epsilon)] &= \sin\theta A[0] + e^{i\epsilon}\cos\theta A[1] \\ &= W\big(\sin\theta\,\mathbb{1} + e^{i\epsilon}\cos\theta\,S(\phi)\big). \end{aligned} \tag{2.9}$$

Here, we have employed the normal form of Eq. (2.7). It is easy to see that the operation in parenthesis (and hence $A[\alpha(\theta,\epsilon)]$) is unitary if and only if $e^{i\epsilon} = \pm 1$.

Here, we are lucky twice. Firstly we have found that whenever there is *one* measurement basis which allows for unitary transport, there is a *one-parameter set* of such bases (corresponding the different values of θ). Secondly, this one-parameter set is closed under passing to the orthogonal measurement outcome

$$\theta \mapsto \pi/2 - \theta, \quad \alpha \mapsto \alpha + \pi.$$

This observation is of sufficient interest to warrant the introduction of a new notation (c.f. Ref. [29])

$$\begin{aligned} |0_\theta\rangle &:= \sin\theta|0\rangle + \cos\theta|1\rangle \\ |1_\theta\rangle &:= \cos\theta|0\rangle - \sin\theta|1\rangle \end{aligned}$$

for the family of bases giving rise to unitary evolution.

Observation 17. *For any computational wire, a measurement in any basis from the*

one-parameter set $\{|0_\theta\rangle, |1_\theta\rangle\}$ *induces a unitary evolution in correlation space.*

We proceed to analyze the operators $A[x_\theta]$. Recall that $A[x_\theta]$ is just *proportional* to a unitary matrix: in general, its operator norm $\|A[x_\theta]\|$ is smaller than one. The norm turns out to have a simple interpretation. Its square specifies the probability with which the operation can be realized.

Lemma 18. *In the limit of large n, the probability of obtaining the outcome $|x_\theta\rangle$ as a result of a local measurement on a quantum wire is given by $\|A[x_\theta]\|^2$.*

Here, "in the limit of large n" means that the statement is true for sites far away from the boundaries of the chain.

Proof. Setting $S = |x_\theta\rangle\langle x_\theta|$ in Eq. (2.39), we find that the relevant probability is given by

$$\mathrm{tr}\left(\mathbb{E}_S(\rho_\infty)\right) = \mathrm{tr}\left(A[x_\theta](1/2\mathbb{1})A[x_\theta]^\dagger\right) = \|A[x_\theta]\|^2.$$

□

Let us take a closer look at the operations

$$A[0_\theta] = 2^{-1/2}\, W\big(\sin\theta\mathbb{1} + \cos\theta S(\phi)\big).$$

The non-trivial bit is the operator in parenthesis

$$U(\theta,\phi) := \sin\theta\mathbb{1} + \cos\theta S(\phi).$$

Clearly, $U(\theta,\phi)$ is a diagonal unitary with eigenvalues

$$\lambda_\pm := \sin\theta + \cos\theta e^{\pm i\phi/2} = \big(\sin\theta + \sin\frac{\phi}{2}\big) \pm i\cos\frac{\phi}{2}, \tag{2.10}$$

visualized in Fig. 2.2.

Let

$$\delta \;=\; \arg(\lambda_+), \qquad p = \mathrm{abs}(\lambda_+)^2,$$

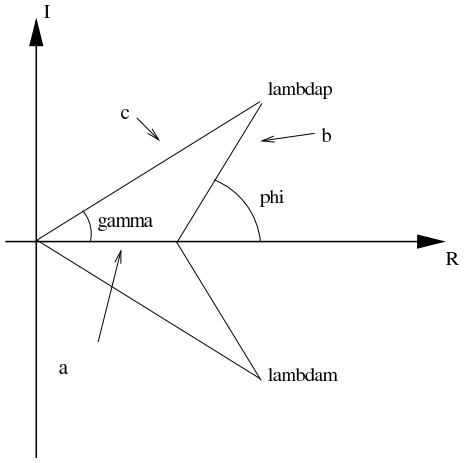


Figure 2.2: Location of the eigenvalues λ_+, λ_- of $U(\theta, \phi)$ in the complex plane. One can read off that $U(\theta, \phi) = c\, S(-2\delta)$.

then $U(\theta, \phi)$ is proportional to $S(-2\delta)$ and can be implemented with probability of success equal to p. We may thus visualize the set of operations one can realize when varying θ by drawing the trajectory of $\lambda_+(\theta, \phi)$ in the complex plane. The result for $\phi = \pi$ and $\phi = \pi/4$ is shown in Fig. 2.3. Apparently, the trajectories are ellipses. This can be verified explicitly:

$$\begin{aligned} & \big(\operatorname{Re} \lambda_+(\theta, \phi), \operatorname{Im} \lambda_+(\theta, \phi) \big)^T \\ = \;& (\sin\theta + \cos\theta \cos\phi/2, \cos\theta \sin\phi/2)^T \\ = \;& \begin{pmatrix} 1 & \cos\phi/2 \\ 0 & \sin\phi/2 \end{pmatrix} \begin{pmatrix} \sin\theta \\ \cos\theta \end{pmatrix}. \end{aligned} \tag{2.11}$$

Varying θ, the final equation describes the image of a circle under a linear transformation (hence an ellipse).

The important lesson to learn is:

Observation 19. *In any computational wire, an* arbitrary phase gate $S(\delta)$ *can be implemented in a single step. The probability of success may depend on* δ.

For the cluster state the corresponding result is well-known. Here, measuring in the $\{|0_\theta\rangle, |1_\theta\rangle\}$-basis results in the operation $HS(\theta)$ on the correlation space. So in this case, the correspondence between the angle θ of the measurement basis and the angle

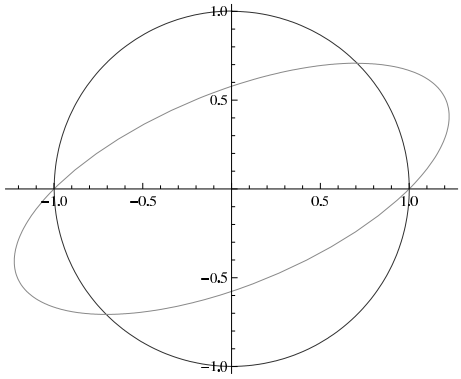


Figure 2.3: Trajectory of all operations for $\phi = \pi$ (circle) and $\phi = \pi/2$ (ellipse). Every point $c\,e^{i\delta}$ on the curve corresponds to the operation $S(-2\delta)$ which can be realized with probability $p = c^2$.

of the correlation space phase gate $S(\theta)$ is trivial. Also, the probability of success does not depend on the phase θ. The same situation clearly holds for general wires with $\phi = \pi$. In all other instances, one must resort to Eqs. (2.10,2.11) in order to work out the relation between γ and θ.

One should take a note that the by-product operator

$$U(\pi/2 - \theta, \phi)U(\theta, \phi)^\dagger$$

does in general depend on θ. It is manifestly equal to $S(\phi)$ only for $\theta = 0$.

Let us dis-regard the issue of randomness for a moment and see which unitary transformations may be implemented in a computational wire after several steps. Obviously, that is the set of unitaries which can be written in the form

$$U = WS(\delta_n)\, WS(\delta_{n-1}) \ldots WS(\delta_1) \tag{2.12}$$

for some n. We claim that whenever Assumption 15 holds, all $U \in SU(2)$ may be approximated arbitrarily well by unitaries of the form in Eq. (2.12).

Proof. Let A be the closure of the set of unitaries of the form in Eq. (2.12). For any $\epsilon > 0$, there is a $k \in \mathbb{N}$ such that $\|W^k - W^\dagger\| < \epsilon$. Hence both $S(\delta)$ and $WS(\delta)W^\dagger$ are in A. Recall that $SU(2) \simeq SO(3)$ and that any rotation can be written as a product of three rotations about any two fixed distinct axes. But $S(\delta)$ corresponds to a rotation

about the Z-axis and $WS(\delta)W^\dagger$ rotates about a different one, as long as Assumption 15 holds. □

It is easily seen that wires not fulfilling Assumption 15 do not allow for universal operations in their correlation spaces. Indeed, if W is diagonal, so is $W\,U(\theta,\phi)$ for all θ,ϕ. If, on the other hand, $W = X$, then all operations in Eq. (2.12) are elements of an infinite dihedral group. Both situations corresponds to proper subgroups of $SU(2)$.

2.2.5 Preparation and read-out

A quantum computation consists of three steps: 1. preparation of the system in a known state, 2. unitary evolution, and 3. readout of the result. We know how to implement the second step in a computational wire, but have yet to address preparation and readout.

Recall the definition

$$|\alpha(\theta,\epsilon)\rangle = \sin\theta|0\rangle + e^{i\epsilon}\cos\theta|1\rangle$$

from Sec. 2.2.4. For $\theta = \pi/4$ and $\epsilon = \phi/2 + \pi$ one finds

$$\begin{aligned} A[\alpha(\pi/4,\phi/2+\pi)] &= \frac{1}{2}W\left(\mathbb{1} - e^{i\phi/2}S(\phi)\right) \\ &= \frac{1}{2}W\left(1 - e^{i\phi}\right)|1\rangle\langle 1|, \end{aligned}$$

which has rank one. Clearly, implementing a rank-one operator on correlation space is equivalent to preparing it in the state proportional to the operator's range (in this case $W|1\rangle$). The operation associated with the orthogonal outcome

$$\begin{aligned} A[\pi/4,\phi/2] &= \frac{1}{2}W\left(\mathbb{1} + e^{i\phi/2}S(\phi)\right) \\ &= \frac{1}{2}W\left(2|0\rangle\langle 0| + (1+e^{i\phi})|1\rangle\langle 1|\right), \end{aligned}$$

has rank one if and only if $\phi = \pi$. Hence in the general case, the preparation procedure may fail to set the correlation system to a definite state. In this case, a new attempt can be started in the next step. The probability of failing to prepare the correlation system successfully is exponentially suppressed in the number of trials.

To prove that read-out is possible, we must show that one can physically decide whether the correlation system is in one of two given orthogonal states $|\phi_0\rangle, |\phi_1\rangle$. This is possible, where again the probability of failing is exponentially small in the number of local sites measured.

Indeed, employing Eq. (2.42), the task is equivalent to distinguishing the two (asymptotically) orthogonal many-body vectors $|\Phi_0\rangle$ and $|\Phi_1\rangle$ by means of local measurements. A well-known result [118] states that this is always possible deterministically.

For short wires, the states $|\Phi_{0/1}\rangle$ may fail to be orthogonal. However, by repeating the computation several times if necessary, it is always efficiently possible to distinguish the two cases.

As an example, consider the T-resource (c.f. Section 2.2.3) with boundary condition $|R\rangle = |0\rangle$. Assume that only one single site has not been measured and that we aim to decide whether the correlation system is in the state $|0\rangle$ or $|1\rangle$. Applying Eq. 2.42 shows that

$$|\Phi_0\rangle = 2^{-1/2}(|0\rangle + |1\rangle), \quad |\Phi_1\rangle = 2^{-1/2}(|0\rangle - i|1\rangle).$$

These two states may be distinguished by means of unambiguous state discrimination with a heralded probability of success of $1/2$ per trial.

2.2.6 Local properties

We can employ Eq. (2.40) to work out the reduced density matrix of a single site in a computational wire. The results are

$$\rho = 1/2 \begin{pmatrix} 1 & \cos\phi/2 \\ \cos\phi/2 & 1 \end{pmatrix} \tag{2.13}$$

for states in the normal form of Theorem 13 and

$$\rho = \begin{pmatrix} \sin^2\gamma & 0 \\ 0 & \cos^2\gamma \end{pmatrix} \tag{2.14}$$

for the normal form given in Theorem 14. Note that the respective always-on operations W, W' do not affect the local properties of the state.

As a quantitative measure of entanglement, we can compute the purity of a single site as a function of ϕ explicitly:

$$\mathrm{tr}(\rho^2) = \frac{1}{4}(3 + \cos\phi) = \sin^4\gamma + \cos^4\gamma$$

(see Fig. 2.4). An intuitive explanation for this behavior has been given in Section 2.2.3.

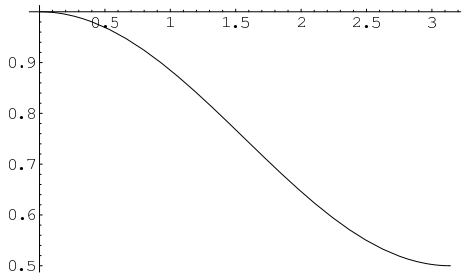


Figure 2.4: Purity of a local site as a function of the by-product angle ϕ.

Observation 20. *Computational wires with arbitrarily low local entanglement exist.*

The density matrices in Eqs. (2.13,2.14) allows us to work out the relationship between the two normal forms Theorem 13, Theorem 14 explicitly. Indeed, the matrix in Eq. (2.13) is diagonal in the $\{|+\rangle, |-\rangle\}$-basis with eigenvalues

$$1/2\,\{1 + \cos(\frac{\phi}{2}), 1 - \cos(\frac{\phi}{2})\} = \{\cos^2(\frac{\phi}{4}), \sin^2(\frac{\phi}{4})\}$$

We find:

Lemma 21. *The two normal forms of Theorem 13 and Theorem 14 are related via the relation $\gamma = \phi/4$ and a basis change of the form*

$$|0\rangle \mapsto |+\rangle, \qquad |1\rangle \mapsto e^{i\alpha}|-\rangle,$$

for a suitable phase α.

2.2.7 Compensating randomness

Due to the presence of by-product operators, there is no way to control which exact operation will be implemented on correlation space as a result of a local measurement.

In order to give a scheme for universal computation, we must devise methods of dealing with the inherent randomness of quantum measurements.

If the always-on term W and the by-product operator $S(\phi)$ generate a finite group, there is a simple and efficient possibility to cope with randomness. This method was first introduced in Chapter 1 and will be sketched briefly below.

Define the *by-product* group to be $\mathcal{B} = \langle W, S(\phi)\rangle$. Measuring several consecutive sites in the computational basis, we effectively implement a random walk on the finite group $\mathcal{B}$ on correlation space. This random walk will visit any element of $\mathcal{B}$ after a finite expected number of steps.

Now assume we want to implement the operation $S(\epsilon)$ on correlation space. Section 2.2.4 provides us with a way of finding an angle θ such that $A[0_\theta] = W\,S(\epsilon)$. The orthogonal outcome will cause $A[1_\theta] = W\,S(\epsilon')$ to act on the correlation space. Assume the first outcome has been obtained. We proceed to measure the following sites in the computational basis, which will implement $W^{-1} \in \mathcal{B}$ after a fixed expected number of steps, leaving us with $W^{-1}WS(\epsilon) = S(\epsilon)$ as desired. In case of a measurement outcome corresponding to $|1_\theta\rangle$, we also teleport the state forward until W^{-1} appears on correlation state. So we have effectively implemented $S(\epsilon')$. One can than re-start the protocol for $S(-\epsilon + \epsilon')$.

By the above paragraph, one can implement $S(\epsilon)$ and any element of $\mathcal{B}$ in a finite expected number of steps. In particular, it is possible to perform $S(\epsilon)$ and $WS(\epsilon)W^\dagger$. But – as long as W is neither diagonal nor equal to X – these two families of unitaries are enough to create any $U \in SU(2)$.

We have seen in Theorem 14 that for any given wire, the always-on operation W and the by-product angle ϕ take on different values in different basis – if one allows for general weights $\sin\gamma, \cos\gamma$ for the defining matrices. So if a wire does not fulfill the above criterion in a given basis, it may still be susceptible to the finite group method by passing to a different basis.

In particular, if a wire given in the normal form of Theorem 14 fulfills the criterion that $\langle W, S(\pi)\rangle$ is finite, then the same is true for the one-parameter family of computational wires with the same always-on operation W but different bias-angles γ.

This observation may be used to construct continuous families of computational

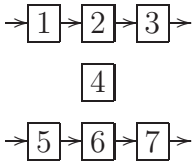
wires in which randomness can be compensated. For example setting $W = H$ with arbitrary γ gives a one-parameter family of deformed cluster states with arbitrarily low local entanglement.

2.3 A coupling scheme

Up to this point, we have analyzed computational wires as "measurement-based analogues of a single qubit". Naturally, all these results are only interesting as long as it is possible to "couple wires together" to form a truly universal resource for measurement-based computation. Fortunately, this can be done.

Here's the physical recipe for coupling the two computational wires defined on sites $\{1, 2, 3\}$ and $\{5, 6, 7\}$ respectively.

In the diagram below, let sites $\{1, 2, 3\}$ and sites $\{5, 6, 7\}$ belong to two computational wires. Assume that a further qubit in the state $2^{-1/2}(|0\rangle + |1\rangle)$ has been placed on site 4.



To entangle the resource, first perform a controlled-Z gate between sites 2 and 4. Then, apply a controlled-Z' gate between 4 and 6. Here, Z' is a Z gate acting in the "preparation basis" (see Section 2.2.5) on site 6:

$$Z' = U\,Z\,U^\dagger, \qquad U = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ e^{i\phi/2} & -e^{i\phi/2} \end{pmatrix}.$$

We need to show that using local measurements, it is possible to either de-couple the wires – i.e. undo the entangling operations to recover the original wires, up to some local corrections – or to implement a logical entangling gate between the correlation systems.

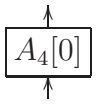
De-coupling is actually trivial: just measure the central site 4 in the computational basis. The two entangling operations above were both controlled unitaries: if the state on the central site is $|0\rangle$, they act as the identity. If, on the other hand, site 4 is in $|1\rangle$, a

Z will be applied to site 2 and a $UZU^\dagger$ to site 6. In particular, the controlled unitaries commute with a measurement in the computational basis on the central site. So if that measurement yields an outcome of $|0\rangle$, we just recover the original wires without any modification. If the outcome is $|1\rangle$, local unitaries act on sites 4 and 6 – which can be counter-acted by a mere change of basis for subsequent measurements.

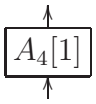
We work out the tensor network representation of the state resulting from the entangling operations. For system 2, set

$$= A[i]_{l\to r} \otimes \langle i|_d,$$

for $i \in \{0, 1\}$. Likewise, for system 4

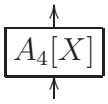


$$= |+\rangle_u \langle +|_d, \quad$$



$$= |-\rangle_u \langle -|_d,$$

so that

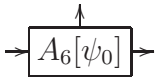


$$= Z^x.$$

Finally, for 6, we first transform into the basis

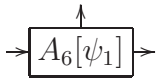
$$\begin{aligned} |\psi\rangle_0 &= U|0\rangle = 1/\sqrt{2}(|0\rangle + e^{i\phi/2}|1\rangle) \\ |\psi\rangle_1 &= U|1\rangle = 1/\sqrt{2}(|0\rangle - e^{i\phi/2}|1\rangle) \end{aligned}$$

to obtain



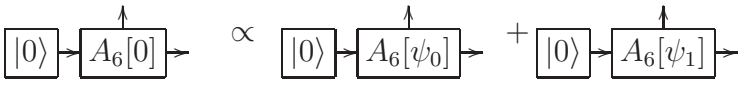
$$\begin{aligned} &= A[\psi_0]_{l\to r} \otimes |0\rangle_u \\ &= \big(\frac{1}{2}W(1-e^{i\phi})|1\rangle_r\langle 1|_l\big) \otimes |0\rangle_u \\ &= \big(W|1\rangle_r\langle 1|_l\big) \otimes \big(\frac{1}{2}(1-e^{i\phi})|0\rangle_u\big), \end{aligned}$$

and, likewise,

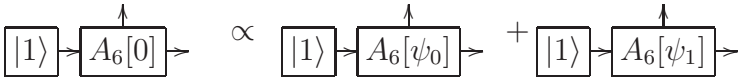


$$\begin{aligned} &= A[\psi_1]_{l\to r} \otimes |1\rangle_u \\ &= \big(W|0\rangle_r\langle 0|_l + \frac{1}{2}(1+e^{i\phi})W|1\rangle_r\langle 1|_l\big) \otimes |1\rangle_u, \\ &= \big(W|0\rangle_r\langle 0|_l\big) \otimes |1\rangle_u + \\ &\quad \big(W|1\rangle_r\langle 1|_l\big) \otimes \big(\frac{1}{2}(1+e^{i\phi})|1\rangle_u\big), \end{aligned}$$

having made use of the computations of Section 2.2.5. We transform back into the computational basis, drop a global factor of $2^{-1/2}$ on the way and consider the result under the input of a computational basis state:

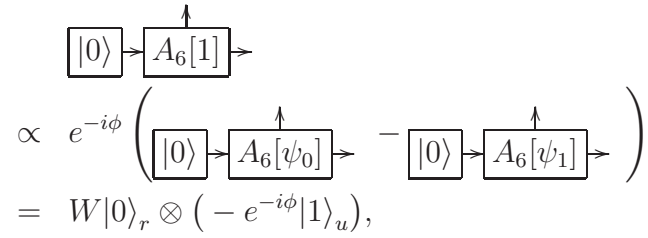


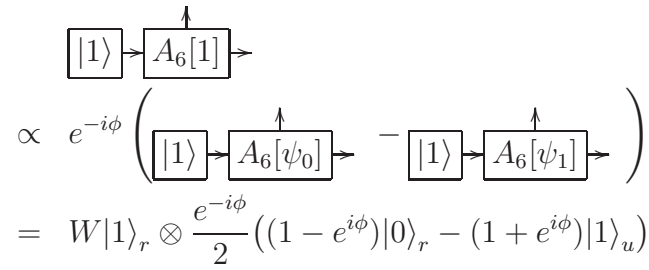
$$= W|0\rangle_r \otimes |1\rangle_u,$$



$$= W|1\rangle_r \otimes \frac{1}{2}\big((1-e^{i\phi})|0\rangle + (1+e^{i\phi})|1\rangle\big)_u,$$

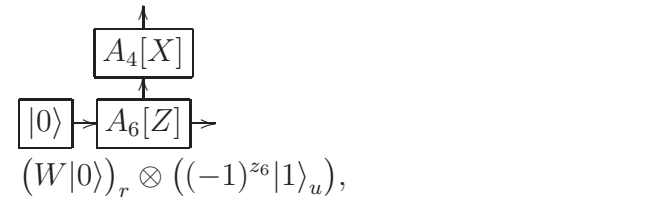
and,



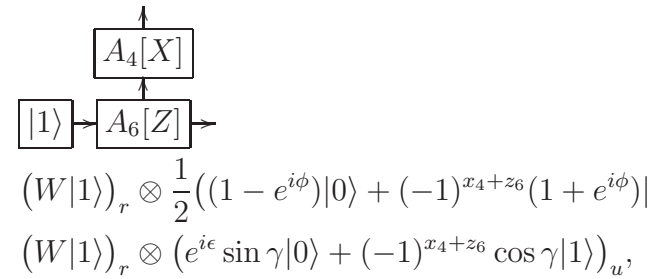


The outputs for the measurement result "0" and "1" differ a) in a global factor of $e^{-i\phi}$ and b) in the application of a Z operator on the upper correlation space. We drop the phase factor a), as it can be gauged away by a local basis change prior to the measurement.

Now, measuring site 6 in the computational basis and site 4 in the X-eigenbasis yields:



(2.15)



(2.16)

for suitable γ, ϵ.

Now, assume $x_4 + z_6$ is even. Choose δ as in Lemma 22. We measure site 2 in the following basis:

$$\psi_0 = (e^{-i\epsilon}\sin\delta, \cos\delta), \qquad \psi_1 = (-e^{-i\epsilon}\cos\delta, \sin\delta).$$

For the first outcome, we get

$$\begin{aligned} |0\rangle_l &\mapsto W|0\rangle \otimes \big(\cos\delta\, A[1]\big), \\ |1\rangle_l &\mapsto W|1\rangle \otimes \big(\sin\delta\sin\gamma\, A[0] + \cos\delta\cos\gamma A[1]\big). \end{aligned}$$

Recall that $A[0] = 2^{-1/2}\mathbb{1}, A[1] = 2^{-1/2}S(\phi)$, and $S(\phi) = \mathrm{diag}(e^{-i\phi/2}, e^{i\phi/2})$. Hence operator

$$\sin\delta\sin\gamma\, A[0] + \cos\delta\cos\gamma A[1]$$

is unitary and has operator norm equal to $2^{-1/2}|\cos\delta|$. The same is obviously true for $\cos\delta\, A[1]$. We conclude that in this particular case, the dynamics in the correlation space is unitary. But by Lemma 22, the same is true for the orthogonal outcome. Also, the case where $x_4 + z_6$ is odd is treated similarly.

We can thus deterministically implement an entangling unitary between the computational wires.

Lemma 22. *For all $\phi, \gamma \in \mathbb{R}$, there is a $\delta \in \mathbb{R}$ such that*

$$|\cos(\delta)| = |\sin(\delta)\sin(\gamma) + \cos(\delta)\cos(\gamma)e^{i\phi/2}|. \tag{2.17}$$

What is more, whenever ϕ, γ, δ fulfill the relation above, it is also true that

$$|\sin(\delta)| = |-\cos(\delta)\sin(\gamma) + \sin(\delta)\cos(\gamma)e^{i\phi/2}|. \tag{2.18}$$

Proof. The first part is obvious: $\delta \mapsto |\cos(\delta)|$ for $\delta \in [0, \pi/2]$ is a continuous function with $|\cos(0)| = 1$ and $|\cos(\pi/2)| = 0$. The right hand side of Eq. (2.17) is also a continuous function, taking values $|\sin(\gamma)|$ and $|\cos(\gamma)|$ at 0 and $\pi/2$, respectively. Hence, the two functions intersect in at least a single point.

To show the second claim compute

$$\begin{aligned}\cos^2(\delta) &= (\sin(\delta)\sin(\gamma)+\cos(\delta)\cos(\gamma)\cos(\phi/2))^2 \\ &+ (\cos(\delta)\cos(\gamma)\sin(\phi/2))^2 \\ &= \sin^2(\delta)\sin^2(\gamma)+\cos^2(\delta)\cos^2(\gamma) \\ &+ 2\sin(\delta)\sin(\gamma)\cos(\delta)\cos(\gamma)\cos(\phi/2). \end{aligned} \tag{2.19}$$

Hence,

$$\begin{aligned}1-\cos^2(\delta) &= (\sin^2(\gamma)+\cos^2(\gamma))(\sin^2(\delta)+\cos^2(\delta)) \\ &- \sin^2(\delta)\sin^2(\gamma)-\cos^2(\delta)\cos^2(\gamma) \\ &- 2\sin(\delta)\sin(\gamma)\cos(\delta)\cos(\gamma)\cos(\phi/2) \\ &= \sin^2(\gamma)\cos^2(\delta)+\cos^2(\gamma)\sin^2(\delta) \\ &- 2\sin(\delta)\sin(\gamma)\cos(\delta)\cos(\gamma)\cos(\phi/2) \\ &= (-\cos(\delta)\sin(\gamma)+\sin(\delta)\cos(\gamma)\cos(\phi/2))^2 \\ &+ (\sin(\delta)\cos(\gamma)\sin(\phi/2))^2 \\ &= |-\cos(\delta)\sin(\gamma)+\sin(\delta)\cos(\gamma)e^{i\phi/2}|^2. \end{aligned} \tag{2.20}$$

This proves the claim. □

2.4 Proofs and technicalities

2.4.1 Qubit channels

We recall some basic facts about qubit channels from Ref. [12, 93]. In what follows, Λ is a (trace-preserving) qubit channel. Viewed as a linear map, we may express it as a matrix with respect to the Pauli basis σ_i, $i = 0, \ldots, 3$. As Λ is trace-preserving (i.e. the dual channel Λ^* is unital), the matrix representation takes the form

$$\mathbf{T} = \begin{pmatrix} 1 & 0 \\ \mathbf{t} & T \end{pmatrix}, \tag{2.21}$$

where $\mathbf{t} \in \mathbb{R}^3$ and T a real 3×3 matrix.

There are unitaries U, V such that the channel

$$\Lambda' : \rho \mapsto V\Lambda(U\rho U^\dagger)V^\dagger \tag{2.22}$$

is represented by

$$\mathbf{T}' = \begin{pmatrix} 1 & 0 & 0 & 0 \\ t_1 & \lambda_1 & 0 & 0 \\ t_2 & 0 & \lambda_2 & 0 \\ t_3 & 0 & 0 & \lambda_3 \end{pmatrix}, \tag{2.23}$$

where $\langle 1, |\lambda_1|, |\lambda_2|, |\lambda_3| \rangle$ are the singular values of T. The channel is unital if and only if $\mathbf{t} = 0$.

Let

$$|\Phi\rangle \;=\; 2^{-1/2}(|00\rangle + |11\rangle). \tag{2.24}$$

The *Choi matrix* of Λ is given by

$$C_\Lambda \;=\; (\Lambda \otimes \mathbb{1}) \left(|\Phi\rangle\langle\Phi|\right) \tag{2.25}$$

It is true [12] that if (a unital) Λ is of the form

$$\Lambda(\rho) = \sum_{i=0}^{3} p_i \, \sigma_i \rho \sigma_i, \tag{2.26}$$

then

$$\mathrm{spec}(C_\Lambda) = \langle p_0, \ldots, p_3 \rangle. \tag{2.27}$$

The *Kraus rank* of a channel Λ is the smallest number k such that

$$\Lambda(\rho) = \sum_{i=1}^{k} A[i] \rho A[i]^\dagger$$

for suitable *Kraus operators* $A[i]$.

Below, we will derive various normal forms for qubit channels of Kraus rank two.

Lemma 23. *Let Λ be a unital qubit channel of Kraus rank two. Then there are unitaries U_0, U_1 and a number $\gamma \in \mathbb{R}$ such that Λ may be represented by means of the Kraus operators*

$$A[0] = \sin\gamma\, U_1, \qquad A[1] = \cos\gamma\, U_2.$$

Note that Lemma 23 is slightly stronger than the well-known known fact that unital qubit channels are random unitary channels (it could a priori be that more unitaries than the Kraus rank of Λ are needed in such a representation).

Proof. Let Λ' be the diagonalized channel as in Eqs. (2.22,2.23). Manifestly, $\operatorname{rank} C_{\Lambda'}$ is not larger than the Kraus rank of Λ'. Using Eqs. (2.26,2.27), one finds

$$\Lambda(\rho) = \sum_{i,p_i\neq 0} p_i (V^\dagger \sigma_i U^\dagger)\rho(V^\dagger\sigma_i U^\dagger)^\dagger, \tag{2.28}$$

which implies the claim. □

We say that two channels Λ_1, Λ_2 are *conjugate* if there exists a unitary U such that

$$\Lambda_1(\rho) = U\Lambda_2(U^\dagger \rho U)U^\dagger$$

for all ρ.[3]

Lemma 24. *Let Λ be a unital qubit channel of Kraus rank two. Then Λ is conjugate to a channel with Kraus operators*

$$A[0] = \sin\gamma\, W, \qquad A[1] = \cos\gamma\, WS(\pi),$$

for $\gamma \in \mathbb{R}$ and $W \in SU(2)$ of the form

$$W = e^{i\sin\alpha/2(\sin\beta X + \cos\beta Z)}. \tag{2.29}$$

[3] Our notion of "being conjugate" coincides with the meaning used in linear algebra. It should not be confused with the way the term is used in Ref. [69]. Channels called "conjugate" in [69] are referred to as "complementary" below, consistent with Ref. [57].

Proof. We read off Eq. (2.28) that Λ can be represented by Kraus operators

$$A[0] = \sin\gamma V^\dagger \sigma_i U^\dagger, \qquad A[1] = \cos\gamma V^\dagger \sigma_j U^\dagger$$

for some $i \neq j$, suitable $U, V \in SU(2)$ and γ such that $\sin^2\gamma = p_i, \cos^2\gamma = p_j$. Conjugating by U, we get

$$\begin{aligned} A'[0] &= \sin\gamma U V^\dagger \sigma_i, \\ A'[1] &= \cos\gamma U V^\dagger \sigma_j = \cos\gamma (U V^\dagger \sigma_i)\, \sigma_i^\dagger \sigma_j. \end{aligned}$$

There exists a unitary X such that $X\sigma_j^\dagger \sigma_i X^\dagger = Z$. Conjugate the primed Kraus operators by X to obtain

$$A''[0] = \sin\gamma W, \qquad A''[1] = \cos\gamma W Z \tag{2.30}$$

for $W = XUV^\dagger X$. As every element of $SU(2)$, W is of the form

$$W = e^{i(r_1 X + r_2 Y + r_3 Z)}$$

for some real unit vector $\mathbf{r}$. Conjugating the $A''[0/1]$'s with a suitable phase gate $S(\epsilon)$, we can set r_2 to zero, without affecting the form of Eq. (2.30). □

Lemma 25. *Let Λ be a unital qubit channel of Kraus rank two. Then Λ is conjugate to a channel with Kraus operators*

$$A[0] = 2^{-1/2} W, \qquad A[1] = 2^{-1/2} W S(\phi)$$

for $\phi \in \mathbb{R}$ and $W \in SU(2)$ of the form

$$W = e^{i \sin\alpha/2 (\sin\beta X + \cos\beta Z)}. \tag{2.31}$$

Note that the unitary W in Lemma 24 and the one in Lemma 25 need not be identical.

Proof. Start with the Kraus operators of Lemma 24. Using the unitary ambiguity of the

Kraus representation, one concludes that

$$\begin{aligned} A'[0] &= W\big(\sin\theta A[0] + \cos\theta A[1]\big), \\ A'[1] &= W\big(\cos\theta A[0] - \sin\theta A[1]\big) \end{aligned} \tag{2.32}$$

is another set of Kraus operators realizing Λ. Because Eq. (2.32) defines a unitary transformation in Hilbert-Schmidt space,

$$\|A'[0]\|_2^2 + \|A'[1]\|_2^2 = \|A[0]\|_2^2 + \|A[1]\|_2^2 = 1.$$

By the intermediate value theorem, there is a value of θ such that $\|A'[0]\|_2^2 = \|A'[1]\|_2^2 = 1/2$.

Set

$$W' = W(\sin\theta\mathbb{1} + \cos\theta S(\pi)).$$

Then $A'[0] = 2^{-1/2}W'$ and

$$\begin{aligned} & A'[1] \\ = \;& 2^{-1/2}\, W'\big[(\sin\theta\mathbb{1} + \cos\theta S(\pi))^{-1}(\cos\theta\mathbb{1} - \sin\theta S(\pi))\big]. \end{aligned}$$

The operator in square brackets is of the form $S(\phi)$ for some ϕ, completing the proof. □

We conclude with two statements relating the normal forms described above to the spectrum of the channel.

Lemma 26. *Let Λ be a unital qubit channel of Kraus rank two. Let γ be the number introduced in Lemma 24. Then the singular values of Λ are 1 and $|\sin^2\gamma - \cos^2\gamma|$, both occurring with multiplicity two.*

Proof. The channel $\Lambda'(\rho) = W^\dagger \Lambda(\rho) W$ maps

$$\begin{aligned} \mathbb{1} &\mapsto \mathbb{1}, \\ Z &\mapsto Z, \\ X &\mapsto (\sin^2\gamma - \cos^2\gamma) X, \\ Y &\mapsto (\sin^2\gamma - \cos^2\gamma) Y, \end{aligned}$$

as can be readily verified. □

Lemma 27. *Let Λ be a qubit channel of Kraus rank not larger than two. Assume the dual channel Λ^* has an eigenvector $A \neq \mathbb{1}$ with eigenvalue λ of absolute value $|\lambda| = 1$. Then Λ is unital. Further, exactly one of the following situation occurs:*

1. *Λ is the identity channel,*
2. *Λ is a non-trivial unitary channel,*
3. *Λ has Kraus rank two. In the language of Lemma 24, one of two possibilities is realized:*
   (a) *W is diagonal. In this case $\lambda = 1$ and the invariant eigenspace of Λ consists of the set of diagonal operators.*
   (b) *$W = X$. It follows that $\lambda = -1$ with unique eigenvector $A = Z$.*

Proof. Let

$$A = \sum_{i=0}^{3} c_i \sigma_i$$

be the expansion of A in the Pauli basis. In the language of Eq. (2.21) the eigenvalue equation $\Lambda^*(A) = \lambda A$ reads

$$\begin{pmatrix} 1 & \mathbf{t} \\ 0 & T^* \end{pmatrix} \mathbf{c} = \lambda\, \mathbf{c}.$$

Hence the trace-less part a

$$a = \sum_{i=1}^{3} c_i \sigma_i$$

of A is an eigenvector of T^* with eigenvalue λ. As the λ_i's appearing in Eq. (2.23) are – up to signs – the singular values of T [93], one has that $|\lambda_i| = 1$ for at least one i. It then follows from the general theory [93] that $t = 0$ and hence that Λ is unital. In particular, the spectrum and the eigenvectors of Λ are the same as the one of Λ^*. Also, Lemmas 24 and 26 are applicable. We will make use of the channel Λ' introduced in the proof of Lemma 26.

We assume first that $(\sin^2\gamma - \cos^2\gamma) = \pm 1$. If the sign is positive, than Λ' is the identity channel. In case of a negative sign, $\Lambda' = X \cdot X$. In either case, Λ is a unitary channel.

Now consider the case where $|\sin^2\gamma - \cos^2\gamma| < 1$. We have that $\|\Lambda'(B)\| \geq \|B\|$ for some operator B if and only if B is a linear combination of $\mathbb{1}$ and Z. Thus, Λ has a non-trivial (i.e. $\neq \mathbb{1}$) eigenvector of absolute value 1 if and only if the channel $W^\dagger \cdot W$ has a non-trivial eigenvector with eigenvalue λ in the space spanned by $\mathbb{1}$ and Z. Since $\mathbb{1}$ is a fixed point, this situation occurs if and only if $W^\dagger Z W = \pm Z$. The positive sign is realized for diagonal operations W. Among the W's of the form given in Lemma 26, the negative sign is possible only for $W = X$. □

2.4.2 MPS tools

In this section, we translate some basic facts about finitely correlated states/MPS from [35] into our language (see also [35]). The basic object of study is the family of MPS of the form

$$|\Psi_n\rangle = \sum_{x_1,\ldots,x_n=0}^{1} \langle R|A[x_n]\ldots A[x_1]|L\rangle \; |x_1,\ldots,x_n\rangle$$

for $A[0/1]$ complex 2×2 matrices. Let us denote the Hilbert space of a physical qubit by $\mathcal{A} \simeq \mathbb{C}^2$ and the correlation space by $\mathcal{B} \simeq \mathbb{C}^2$.

Clearly,

$$\begin{aligned} & |\Psi_n\rangle\langle\Psi_n| \\ = & \sum_{\mathbf{x},\mathbf{y}} \langle R|A[x_n]\ldots A[x_1]|L\rangle \, \langle L|A[y_1]^\dagger \ldots A[y_n]^\dagger|R\rangle \\ & |x_1\rangle\langle y_1| \otimes \cdots \otimes |x_n\rangle\langle y_n|. \end{aligned} \tag{2.33}$$

It is always possible to find matrices $A[0], A[1]$ and boundary conditions $|L\rangle, |R\rangle$ such that

$$A[0]^\dagger A[0] + A[1]^\dagger A[1] = \mathbb{1} \tag{2.34}$$

without changing the state $|\Psi_n\rangle$ [84]. We will assume this normal form from now on. Define $V : \mathcal{B} \to \mathcal{A} \otimes \mathcal{B}$ by

$$V = |0\rangle_{\mathcal{A}} \otimes A[0]_{\mathcal{B}} + |1\rangle_{\mathcal{A}} \otimes A[1]_{\mathcal{B}}.$$

It follows that

$$V^\dagger V = A[0]^\dagger A[0] + A[1]^\dagger A[1] = \mathbb{1},$$

so that V is an isometry. It holds that

$$V|L\rangle\langle L|V^\dagger = \sum_{x_1,y_1} |x_1\rangle\langle y_1| \otimes A[x_1]|L\rangle\langle L|A[y_1].$$

Plugging the preceding formula recursively into Eq. (2.33), we get

$$\begin{aligned} & |\Psi_n\rangle\langle\Psi_n| \\ = \; & \langle R|V \dots V|L\rangle\langle L|V^\dagger \dots V^\dagger|R\rangle \\ = \; & \mathrm{tr}_{\mathcal{B}} \left(|R\rangle\langle R| \, V \dots V|L\rangle\langle L|V^\dagger \dots V^\dagger \right). \end{aligned}$$

Now, let S_i be an observable on the ith copy of $\mathcal{A}$. Define

$$\begin{aligned} \mathbb{E}_{S_i}(\rho) \; &:= \; \mathrm{tr}_{\mathcal{A}} \left(S_i V \rho V^\dagger \right) \\ &= \; \sum_{x_i,y_i} \left(\langle y_i|S_i|x_i\rangle \right) A[x_i]\rho A[y_i]^\dagger \end{aligned}$$

and, in particular,

$$\hat{\mathbb{E}}(\rho) := \mathbb{E}_{\mathbb{1}}(\rho) = \sum_x A[x]\rho A[x]^\dagger. \tag{2.35}$$

The super-operators $\mathbb{E}_{S_i}$ allow us to compute expectation values as in

$$\begin{aligned} & \operatorname{tr}\left(S_1 \otimes \cdots \otimes S_n \, |\Psi_n\rangle\langle\Psi_n|\right) \\ = \; & \operatorname{tr}_{\mathcal{B}}\left(|R\rangle\langle R| \, \mathbb{E}_{S_n} \ldots \mathbb{E}_{S_1}(|L\rangle\langle L|)\right). \end{aligned} \tag{2.36}$$

Equation (2.35) shows manifestly that $\hat{\mathbb{E}}$ is a quantum channel. By Eq. (2.34), $\mathbb{1}$ is an eigenvector of the dual channel

$$\hat{\mathbb{E}}^*(X) = \sum_x A[x]^\dagger X A[x]$$

with eigenvalue 1 (meaning that $\hat{\mathbb{E}}$ is trace-preserving).

We now distinguish two cases:

1. The map $\hat{\mathbb{E}}^*$ has a spectral gap. Hence $\mathbb{1}$ is the only eigenvector with an eigenvalue of absolute value 1.

2. There is an eigenvector $A \neq \mathbb{1}$ of $\hat{\mathbb{E}}^*$ with eigenvalue λ of absolute value $|\lambda| = 1$.

The theory of MPS is much better-behaved in the first case [35] on which we will concentrate in what follows. This does not sacrifice too much generality: Lemma 27 gives a complete classification of the set of measure zero for which $\hat{\mathbb{E}}$ does not have a spectral gap.

Restricting attention to case 1. above, note that $\operatorname{spec}(\hat{\mathbb{E}}) = \operatorname{spec}(\hat{\mathbb{E}}^*)^*$, and that right-eigenvectors of $\hat{\mathbb{E}}$ are left-eigenvectors of $\hat{\mathbb{E}}^*$ and vice-versa. It follows that there is a unique invariant state ρ_∞ of $\hat{\mathbb{E}}$ and further that

$$\hat{\mathbb{E}}^n(|L\rangle\langle L|) \to \operatorname{tr}(|L\rangle\langle L|)\, \rho_\infty \tag{2.37}$$

exponentially fast as $n \to \infty$.

Now, choose the normalization of $|L\rangle, |R\rangle$ such that

$$\operatorname{tr}\left(|L\rangle\langle L|\right) = 1, \qquad \operatorname{tr}\left(|R\rangle\langle R| \, \rho_\infty\right) = 1. \tag{2.38}$$

Employing Eq. (2.36) we find that

$$\begin{aligned} & \lim_{n\to\infty} \operatorname{tr}\left(|\Psi_n\rangle\langle\Psi_n|\right) \\ = & \lim_{n\to\infty} \operatorname{tr}\left(|R\rangle\langle R|\,\hat{\mathbb{E}}^n(|L\rangle\langle L|)\right) \\ = & \operatorname{tr}\left(|R\rangle\langle R|\,\rho_\infty\right)\operatorname{tr}(|L\rangle\langle L|) = 1, \end{aligned}$$

so that the choice (2.38) is asymptotically compatible with the requirement that $|\Psi_n\rangle$ be normalized.

We continue by computing

$$\begin{aligned} & \lim_{n\to\infty} \operatorname{tr}\left(\mathbb{1}^{\otimes n} \otimes S \otimes \mathbb{1}^{\otimes n}\,|\Psi_{2n+1}\rangle\langle\Psi_{2n+1}|\right) \qquad (2.39) \\ = & \operatorname{tr}\left(\mathbb{E}_S(\rho_\infty)\right). \end{aligned}$$

Hence, manifestly, the outcomes of measurements on sites sufficiently far away from the boundaries of the chain *do not depend on the boundary conditions* $|L\rangle, |R\rangle$. What is more, their influence is suppressed exponentially fast in the distance to the boundary. We may thus speak of "the state associated with the matrices $A[0], A[1]$".

Setting $S = |i\rangle\langle j|$, one can use Eq. (2.39) to derive the reduced density matrix ρ of a single site in the chain:

$$\begin{aligned} \rho &= \operatorname{tr}_{[-n,-1],[1,n]}\,|\Psi_{2n+1}\rangle\langle\Psi_{2n+1}| \qquad (2.40) \\ &\to \frac{1}{2}\sum_{i,j} \operatorname{tr}\left(A[i]^\dagger A[j]\right)|i\rangle\langle j| \qquad (2.41) \end{aligned}$$

as $n \to \infty$.

Lastly, let

$$\rho_\infty = \lambda_1|\phi_1\rangle\langle\phi_1| + \lambda_2|\phi_2\rangle\langle\phi_2|$$

be the spectral decomposition of the invariant state. As a consequence of Eq. (2.36) one finds that

$$\operatorname{tr}_{[n/2+1,\ldots n]}\,|\Psi_n\rangle\langle\Psi_n| \to \lambda_1^2|\Phi_1\rangle\langle\Phi_1| + \lambda_2^2|\Phi_2\rangle\langle\Phi_2|$$

as $n \to \infty$. Here,

$$|\Phi_i\rangle = \sum_{x_1,\ldots,x_{n/2}=0}^{1} \langle R|A[x_n]\ldots A[x_1]|\phi_i\rangle \ |x_1,\ldots,x_n\rangle. \tag{2.42}$$

One may easily check that the $|\Phi_i\rangle$'s are (asymptotically) normalized. It is also true that the $|\Phi_0\rangle$ is (asymptotically) orthogonal to $|\Phi_1\rangle$. Indeed, by Eq. (2.37), $\hat{\mathbb{E}}^n$ converges to the completely depolarizing channel as $n \to \infty$. By Theorem 3 of [73], the complementary channel converges to the noiseless channel. But $|\Phi_i\rangle$ is just the output of that complementary channel acting on $|\phi_i\rangle$. Because the $|\phi_i\rangle$'s are orthogonal, so must the $|\Phi_i\rangle$.

Clearly then, the entropy of entanglement between the two half-chains converges to one bit if and only if

$$\lambda_1 = \lambda_2 \ \Leftrightarrow \ \rho_\infty \propto \mathbb{1}.$$

Thus:

Proposition 28. *If $\hat{\mathbb{E}}$ has a spectral gap, then the entropy of entanglement between two half-chains is maximal if and only if $\hat{\mathbb{E}}$ is unital.*

3

Too entangled to be useful: measurement-based computation on generic states

3.1 Introduction

A classical computer endowed with the power to perform measurements on certain entangled many-body states is thought to be exponentially more powerful than a classical machine alone. For example, a computer with access to local measurements on a cluster state can find factors of a large integer in an amount of time polynomial in the number of digits of that integer [82, 102]. The best-known classical algorithm requires super-polynomial runtime and it is strongly believed that no substantial improvement is possible. It is in this sense that certain many-body states possess strong computational powers.

How common is this property? There are at least two reasons for believing that typical pure quantum states are powerful resources.

Firstly, this belief may be based on an intuition akin to Feynman's famous argument: because simulating quantum mechanics seems to be too hard for a classical computer, it must conversely be true that the laws of quantum mechanics offer superior computational power. Now, predicting the results of local measurements even on a quantum state which has a simple classical characterization (e.g. in terms of a preparation procedure, or a local Hamiltonian for which it is the ground state) is tremendously difficult in general. What is more, a typical state is described by exponentially many parameters – so it cannot even be efficiently represented in the memory of a classical computer, let alone be subject to an efficient simulation. One would hence expect it to be a potent computational resource, if only a suitable scheme could be devised to utilize its power.

Secondly, one may recall that generic states are extremely highly entangled from many points of view [53]. For example, a typical state is an excellent resource for quantum teleportation with respect to any partition of its systems into two parties. Why then shouldn't such a state also be an equally excellent resource for measurement-based computation? What is more, all previous results (the author is aware of) which rule out universality for certain states do so by proving that the states *are not entangled enough* to support a universal quantum calculation [79, 108, 109].

Both arguments turn out to be fallacies. We show below that families of states with a very high *geometric measure* of entanglement cannot be universal. Recall that the

geometric measure [9, 101, 122] of a state vector $|\Psi\rangle$ is defined as

$$E_g(|\Psi\rangle) = -\log \sup_{\alpha} |\langle\alpha|\Psi\rangle|^2,$$

the supremum being over all product vectors $|\alpha\rangle$.[1] We proceed to show that the criterion is fulfilled by generic states: they are too entangled to be useful in this sense. The fraction of n qubit states subject to this problem will be shown to be at least $1 - e^{-n^2}$.

The intuition behind the argument is that most states are so "skew" to the set of product states, that the results of local measurements convey very little information. The (mild) technical difficulty one needs to overcome in order to make the statement rigorous, is to establish that for most given states, *any* possible measurement scheme fails to yield useful information – even if one has complete knowledge about the state and the capability of adjusting future measurement bases conditioned on previous outcomes.

The observations presented in this chapter should be interesting in the context of the broad question asking to which extend "entanglement" is responsible for a quantum computational speed-up [65].

3.2 Statement of results

We will show that certain highly entangled states cannot enhance the power of a classical computer to solve NP problems. (For definiteness, one may think of the paradigmatic factoring problem.)

Theorem 29 (Classical simulation of highly entangled states)**.** *Let $|\Psi_n\rangle$ be an n qubit state with geometric measure of entanglement*

$$E_g(|\Psi_n\rangle) > n - \delta.$$

Consider a classical computer which has the power to perform local measurements on $|\Psi_n\rangle$. Assume this joint system is capable of finding a solution to an NP *problem P after t time steps, with probability of success at least $1/2$.*

[1] In this chapter, $\log$ is the base 2 logarithm and $\ln$ the natural logarithm.

Then there exists a purely classical *algorithm which identifies a solution to P after*

$$2C(n) \ln \frac{1}{p_f} 2^{\delta}$$

time steps with probability of success at least $1 - p_f$. Here, $C(n)$ is the time it takes to verify that a proposed solution to P is valid.

Note that C is a polynomial function of n (this being the defining property of NP problems).

The theorem implies that a family of states $|\Psi_n\rangle$ cannot provide a super-polynomial speedup whenever their geometric measure is of the form $E_g(|\Psi_n\rangle) = n - O(\log n)$. A priori it is unclear that states with such an extreme geometric entanglement exist at all. It turns out that not only do they exist, but that this property is shared by the vast majority of all many-body states.

Theorem 30 (Typical geometric entanglement)**.** *The fraction of state vectors on $n \geq 11$ qubits with geometric measure of entanglement less than $(n - 2 \log n - 3)$ is smaller than e^{-n^2}.*

Corollary 31 (MBQC-uselessness is typical)**.** *Use the notions of Theorem 29. The fraction of pure states on n qubits which have the power to speed up a classical computer by more than a factor of*

$$16C(n) \ln \frac{1}{p_f} n^2$$

is smaller than e^{-n^2}.

Can we thus conclude that families of highly entangled states are not universal for measurement-based quantum computing? The answer is "yes", up to a standard assumption. Indeed, Theorem 29 pertains only to NP problems. While highly unlikely, there is currently no way of ruling out that quantum computers offer super-polynomial speedups over their classical counterparts for some problems, but fail to do so for any problem in NP. Recall, however, that Shor's algorithm [102] assures that quantum computers can factor integers in polynomial time. It is very strongly suspected that classical machines alone require super-polynomial time for the same task.

Therefore, it is extremely reasonable to assume that there is some NP problem for which quantum computation offers a super-polynomial speedup (so NP $\cap$ BQP $\neq$ BPP [121]).[2] Under this assumption, we may state:

Theorem 32 (Criterion for MBQC-uselessness)**.** *Let $\{|\Psi_n\rangle\}_n$ be a family of quantum states, where $|\Psi_n\rangle$ is defined on n qubits. If*

$$E_g(|\Psi_n\rangle) > n - O(\log n),$$

then the family is not universal for measurement-based computation.

3.3 Proofs

Proof of Theorem 29. We assume that the classical part of the algorithm is deterministic. This entails no loss of generality, since any probabilistic parts may be implemented by using quantum measurements as coins.[3] In the course of the calculation, the computer will perform up to n local measurements, obtaining one of 2^n possible sequences of outcomes. There is a set G of "good" outcomes, which will cause the computer to output a valid solution to the problem P after t time steps. By assumption, the probability of obtaining an outcome from the set G is larger than $1/2$. Each element of G is labeled by a product state $|\alpha\rangle$ in the obvious way. Clearly, the probability of the event associated with $|\alpha\rangle$ to occur is

$$|\langle\alpha|\Psi\rangle|^2 \leq 2^{-E_g\left(|\Psi\rangle\right)} \leq 2^{-n+\delta}.$$

Hence

$$1/2 \leq \mathrm{Prob}(G) < |G|\, 2^{-n+\delta} \quad \Rightarrow \quad |G| > 2^{n-\delta-1}.$$

Thus the ratio of good outcomes to the total number obeys $|G|/2^n > 2^{-\delta-1}$.

[2] Failure of this assumption to hold would result in far more profound problems for the field of quantum information theory than the existence of a vacuous statement in a PhD thesis.

[3] In fact, this seems to be the only way to introduce true randomness into an otherwise classical (and hence deterministic) setup.

To simulate the procedure on a classical probabilistic computer, use the following algorithm: Choose the outcome of the measurements randomly using a fair coin. If the random string causes the classical part of the computation to output a result after t time steps, check whether it solves the problem P. If the result is valid, output it and abort. Otherwise – or if the computer fails to terminate after t time steps – repeat the procedure with another random string.

The probability of not having obtained a valid outcome after k trials is bounded above by

$$(1 - 2^{-\delta-1})^k < e^{-k\,2^{-\delta-1}}.$$

Set $k = \ln(1/p_f)2^{\delta+1}$ to achieve a probability of failure smaller than p_f. The claim is now immediate. □

Lemma 33 (Measure concentration on the sphere)**.** *Let $|\alpha\rangle$ be a normalized vector in $\mathbb{C}^d$, let $|\Psi\rangle$ be drawn from the unit sphere according to Haar measure. Then*

$$\mathrm{Prob}\{|\langle\alpha|\Psi\rangle|^2 \geq \epsilon\} < \exp\{-(2d-1)\epsilon\}.$$

Proof. The cumulative distribution function

$$\mathrm{Prob}\{2d\,|\langle\alpha|\Psi\rangle|^2 \geq x\} = \left(1 - \frac{x}{2d}\right)^{2d-1}$$

can be found in [56, 86] (the factor 2 in front of the dimension is a result of working in a complex space as explained in the appendix). We set $\epsilon = x/(2d)$ and compute

$$(1-\epsilon)^{2d-1} = \exp\{\ln(1-\epsilon)(2d-1)\} \leq \exp\{-\epsilon(2d-1)\},$$

having made use of the concavity of $\ln$. □

Lemma 34 (Nets)**.** *On the set of pure product states on k qubits, there is an ϵ-net $\mathcal{N}_{\epsilon,k}$ where*

$$|\mathcal{N}_{\epsilon,k}| \leq \left(\frac{5k}{\epsilon}\right)^{4k}.$$

More specifically,

$$\sup_{\alpha} \inf_{\tilde{\alpha}} \left|\left||\alpha\rangle - |\tilde{\alpha}\rangle\right|\right|_2 < \epsilon/2 \tag{3.1}$$

$$\Rightarrow \quad \sup_{\alpha} \inf_{\tilde{\alpha}} \left|\left||\alpha\rangle\langle\alpha| - |\tilde{\alpha}\rangle\langle\tilde{\alpha}|\right|\right|_1 < \epsilon \tag{3.2}$$

$$\Leftrightarrow \quad \sup_{\alpha} \sup_{\tilde{\alpha}} |\langle\alpha|\tilde{\alpha}\rangle|^2 \geq 1 - \frac{\epsilon^2}{4}, \tag{3.3}$$

where the optimizations are over all product states $|\alpha\rangle$ and all elements $|\tilde{\alpha}\rangle$ of the net $\mathcal{N}_{\epsilon,k}$.

Proof. For the second part, see Lemma II.4 in [52] (see also Ref. [77]).

As for the first part, let $|\alpha_i\rangle \in \mathbb{C}^2$ such that $|\alpha\rangle = \bigotimes_i |\alpha_i\rangle$. Let $\mathcal{M}$ be an (ϵ/k)-net in the set of qubit states. Hence, for every i, there exists $|\tilde{\alpha}_i\rangle \in \mathcal{M}$, such that

$$|\langle\alpha_i|\tilde{\alpha}_i\rangle|^2 \geq 1 - \frac{\epsilon^2}{4k}.$$

It follows that

$$|\langle\alpha|\tilde{\alpha}\rangle|^2 \geq \left(1 - \frac{\epsilon^2}{4k}\right)^k \geq 1 - \frac{\epsilon^2}{4},$$

where the final inequality can be checked by differentiating with respect to k.

To conclude, set $\mathcal{N}_{\epsilon,k}$ to be the set of all k-fold tensor products of elements in $\mathcal{M}$ and use the upper bound for the cardinality of $\mathcal{M}$ from [52]. □

Proof of Theorem 30. Let $\epsilon = 2^{-l}$ for some yet to be determined number l. Let $\mathcal{N}_{\epsilon,n}$ be an ϵ-net on the set of product vectors on n qubits. By Lemma 33 and the union bound,

$$\begin{aligned}
&\mathrm{Prob}\{\sup_{|\tilde{\alpha}\rangle \in \mathcal{N}_{\epsilon,n}} |\langle\tilde{\alpha}|\Psi\rangle|^2 \geq 2^{-l}\} \\
< \;& \exp\{-(2^{n+1}-1)2^{-l}\} \left|\mathcal{N}_{\epsilon,n}\right| \\
< \;& \exp\{-2^{n-l} + 2nl\ln 2 + 4n\ln(5n)\} \\
< \;& \exp\{-2^{n-l} + 2nl\} \qquad (3.4) \\
< \;& \exp\{-2^{n-l} + 2n^2\} \qquad (3.5)
\end{aligned}$$

where the estimate (3.4) is valid if

$$2nl(1 - \ln 2) > 4\ln(5n). \tag{3.6}$$

Choosing $l = n - \log(3n^2)$, the condition above is satisfied when $n \geq 11$. Further, Eq. (3.5) becomes $\exp\{-n^2\}$.

Now let $|\alpha\rangle$ be a general product vector and $|\tilde{\alpha}\rangle$ be the closest element in the ϵ-net. Then

$$\begin{aligned} \left| |\langle\alpha|\Psi\rangle|^2 - |\langle\tilde{\alpha}|\Psi\rangle|^2 \right| &= \left| \operatorname{tr}\left((|\alpha\rangle\langle\alpha| - |\tilde{\alpha}\rangle\langle\tilde{\alpha}|)|\Psi\rangle\langle\Psi| \right) \right| \\ &\leq \left|\left| |\alpha\rangle\langle\alpha| - |\tilde{\alpha}\rangle\langle\tilde{\alpha}| \right|\right|_\infty \\ &\leq \left|\left| |\alpha\rangle\langle\alpha| - |\tilde{\alpha}\rangle\langle\tilde{\alpha}| \right|\right|_1 \\ &\leq \epsilon = 2^{-l}. \end{aligned}$$

It follows that

$$\sup_{|\alpha\rangle} |\langle\alpha|\Psi\rangle|^2 \leq 2^{-l+1} = 2^{-n+2\log n+\log 3+1} < 2^{-n+2\log n+3}$$

with probability larger than $1 - e^{-n^2}$. □

The proofs of Corollary 31 and Theorem 32 should now be obvious.

3.4 Outlook

The results sketched in this chapter can be greatly strengthened. For example, one can show that typical states still fail to be universal in some sense, even if one assumes nature would allow us to *choose* the outcomes of local measurements should we so desire. While this scenario is incredibly powerful for some states (linked to the complexity class PostBQP $=$ PP [1]), it turns out that postselected measurements on typical states once more fail to allow for universal measurement-based computation in some sense.

3.5 Appendix: Real vs. complex vector spaces

The proof of Lemma 33 depends on a concentration phenomenon of the Haar measure on *real* spheres [56, 86]. Obviously, we are concerned with state vectors drawn from a *complex* d-sphere. In this section, we will briefly state the relation between the respective notions of Euclidean distance and Haar measure on the real and complex sphere.

Suppose $x \in \mathbb{C}^d$ is of the form $a + ib$ for $a, b \in \mathbb{R}^d$. We use the usual ($\mathbb{R}$-linear) mapping

$$\iota : x \mapsto \begin{pmatrix} a \\ b \end{pmatrix}$$

from $\mathbb{C}^d$ to $\mathbb{R}^{2d}$. Then

$$\begin{aligned} & \langle x, x' \rangle && (3.7) \\ = \; & \langle a, a' \rangle - i\langle b, a' \rangle + i\langle a, b' \rangle + \langle b, b' \rangle && (3.8) \\ = \; & \big(\iota(x), \iota(x')\big) + i\big[\iota(x), \iota(x')\big], && (3.9) \end{aligned}$$

where $\langle \cdot, \cdot \rangle$ is the canonical scalar product in $\mathbb{C}^d$, $(\cdot, \cdot)$ the Euclidean one in $\mathbb{R}^{2d}$ and $[\cdot, \cdot]$ the symplectic product in $\mathbb{R}^{2d}$. In particular,

$$\langle x, x \rangle = (x, x) \quad \Rightarrow \quad \|x\|_{\mathbb{C}^d} = \|\iota(x)\|_{\mathbb{R}^{2d}}.$$

Hence ι preserves Euclidean distances.

Now define a measure $\mu_{\mathbb{C}}$ on $\mathbb{C}^d$ in terms of the Haar measure $\mu_{\mathbb{R}}$ by

$$\mu_{\mathbb{C}}(A) = \mu_{\mathbb{R}}(\iota(A)).$$

From Eq. (3.9) it is clear that the effect of a unitary operation on A corresponds to an orthogonal and symplectic operation on $\iota(A)$. Hence $\mu_{\mathbb{C}}$ is $U(d)$-invariant and must thus be the Haar measure.

Part II

Discrete phase spaces

3.6 Introduction

The term *phase space* originates in classical mechanics. Here, the state of a single particle in one spatial dimension is completely specified by two real parameters: its position and its momentum. The two-dimensional real vector space spanned by the position and the momentum axes is referred to as the particle's phase space. Likewise, the state of a single continuous-value quantum system may be specified by a quasi-probability distribution on phase space – namely the particle's Wigner function.

The Wigner function shares many properties of classical probability distributions, except for the fact that it can take negative values. Quantum phase space methods are employed heavily in some areas of physics, such as quantum optics [95], the investigation of a "quantum-classical correspondence" [66, 124], or representation theory of the canonical commutation relations [36, 85], to name a few.

Considerable work has been undertaken to explore Wigner functions for finite-dimensional quantum systems [24, 39, 46, 71, 74, 78, 94, 116, 117, 126]. It is fair to say that discrete phase space tools have been studied mainly for their mathematical appeal. The author is not aware of any technical problem that has been solved using discrete Wigner functions that could not – or only in a considerably less convenient way – have been treated without resorting to phase space methods (see, however, Chapter 5).

In **Chapter 4** we give an in-depth introduction into discrete quantum phase spaces. Beyond the Wigner function as such, we treat a whole array of related structures such as Weyl-Heisenberg operators (or generalized Pauli operators), the Clifford group, and stabilizer states. All these mathematical objects fit seamlessly into the phase space formalism.

The analogy between Wigner functions and probability-distributions is spoiled by the fact that the former may become negative. It is hence natural to ask whether there are quantum states for which this problem does not occur. The main technical result of Chapter 4 pertains to this question: We show that, on a Hilbert space of odd dimension, the only pure states to possess a non-negative Wigner function are stabilizer states. The Clifford group is identified as the set of unitary operations which preserve positivity. The result can be seen as a discrete version of Hudson's Theorem. Hudson established

that for continuous variable systems, the Wigner function of a pure state has no negative values if and only if the state is Gaussian. Turning to mixed states, it might be surmised that only convex combinations of stabilizer states give rise to non-negative Wigner distributions. We refute this conjecture by means of a counter-example.

Chapter 5 presents a technical application of the methods derived before. We use it to quantize the Margulis expander map – a well-known structure in classical computer science. The result is a quantum expander which acts on discrete Wigner functions in the same way the classical Margulis expander acts on probability distributions. The construction is the only instance known to the author where finite phase space techniques facilitate the simple solution of an otherwise non-trivial problem. What is more, applications based on discrete and continuous phase spaces can be developed in complete analogy.

4

A discrete Hudson’s theorem

4.1 Introduction

4.1.1 General Introduction

The Wigner distribution establishes a correspondence between quantum mechanical states and real pseudo-probability distributions on phase space. 'Pseudo' refers to the fact that, while the Wigner function resembles many of the properties of probability distributions, it can take on negative values. This phenomenon has been linked to non-classical features of such quantum states (see Ref. [66] for an exposition of literature on that problem). It is naturally of interest to characterize those quantum states that are classical in the sense of giving rise to non-negative phase space distributions.

For the case of pure states described by vectors in $\mathcal{H} = L^2(\mathbb{R})$, the resolution of this problem was given by Hudson in Ref. [60]. Later, Soto and Claverie generalized Hudson's result to states of multi-particle systems (Ref. [104]).

Theorem 35. (Hudson, Soto, Claverie) *Let $\psi \in L^2(\mathbb{R}^n)$ be a state vector. The Wigner function of ψ is non-negative if and only if ψ is a* Gaussian state.

By definition, a vector is Gaussian if and only if it is of the form

$$\psi(q) \propto e^{2\pi i(q\theta q + xq)},$$

where $q, x \in \mathbb{R}^n$ and θ is a symmetric matrix with entries in $\mathbb{C}$ [1].

It is our objective to prove that the situation for discrete quantum systems is very similar, at least when the dimension of the Hilbert space is odd. Before stating the result, we pause for a brief overview of its main ingredients: discrete Wigner functions and stabilizer states.

The Wigner function [125] of a pure state $\psi \in L^2(\mathbb{R})$ is computed as

$$W_\psi(p,q) = \pi^{-1} \int_{\xi \in \mathbb{R}} e^{-2\pi i \xi p}\, \bar{\psi}(q - \frac{1}{2}\xi)\psi(q + \frac{1}{2}\xi). \tag{4.1}$$

Equivalently, W_ψ is the (symplectic) Fourier transform of the *characteristic function*

[1] Note that the boundedness of $\psi \in L^2(\mathbb{R}^n)$ implies that θ has positive semi-definite imaginary part.

Ξ_ψ, which in turn is defined by

$$\Xi_\psi(p,q) = \mathrm{tr}(w(p,q)^\dagger |\psi\rangle\langle\psi|).$$

Here, $w(p,q) = e^{i(p\hat{X} - q\hat{P})}$ are the well-known *Weyl* or *displacement operators* [36, 119]. Partly triggered by the advent of quantum information theory, considerable work has been undertaken to explore Wigner functions for finite-dimensional quantum systems [24, 39, 46, 71, 74, 78, 94, 116, 117, 126]. Two approaches might be identified in the literature on that subject. The first one aims to cast the *definition* of the Wigner function into a form that can be interpreted for both continuous variable and discrete systems [46, 78, 116, 117]. The second approach – introduced by Gibbons, Hoffman, and Wootters in Ref. [39] – focuses on the *properties* of Eq. (4.1). The authors imposed a set of axioms which a candidate definition of a discrete Wigner function would have to fulfill in order to resemble the well-known continuous counterpart.

We will argue that, for odd dimensions d,

$$W_\psi(p,q) = d^{-1} \sum_{\xi \in \mathbb{Z}_d} e^{-\frac{2\pi}{d} i \xi p}\, \bar{\psi}(q - 2^{-1}\xi)\psi(q + 2^{-1}\xi)$$

is the most sensible analogue of Eq. (4.1), judged in terms of either of these approaches. Here, p, q are elements of $\mathbb{Z}_d = \{0, \ldots, d-1\}$ and $2^{-1} = (d+1)/2$ is the multiplicative inverse of 2 modulo d. Indeed, the definition given above is the discrete symplectic Fourier transform of the discrete characteristic function and will be shown to be the *unique* choice to mimic certain desirable properties of the continuous Wigner function.

Stabilizer states were originally defined by Gottesman in Ref. [40] as the joint eigenvectors of certain sets of elements of the qubit Pauli group. Exceeding the case of qubits, stabilizer states for higher-dimensional quantum systems have been treated in the literature (see, e.g. Refs. [42, 59, 72, 96]). Such states find manifold applications in quantum information theory, ranging from quantum error correction [82] to Cluster state quantum computation [91]. Although displaying complex features such as multi-particle entanglement [55], stabilizer states allow for an efficient classical description. In particular, a quantum computer that operates only with stabilizer states can offer no principal advantage over classical methods of computing [82]. The latter statement is sometimes called

Gottesman-Knill Theorem.

Using that language, we intend to show:

Theorem 36. (Discrete Hudson's Theorem) *Let d be odd and $\psi \in L^2(\mathbb{Z}_d^n)$ be a state vector. The Wigner function of ψ is non-negative if and only if ψ is a* stabilizer state.

Given that $\psi(q) \neq 0$ for all q, a vector ψ is a stabilizer state if and only if it is of the form

$$\psi(q) \propto e^{\frac{2\pi}{d} i(q\theta q + xq)},$$

where $q, x \in \mathbb{Z}_d^n$ and θ is a symmetric matrix with entries in $\mathbb{Z}_d$.

Theorem 36 should convey two central messages. Firstly, if the right definitions are employed, the continuous and the discrete case behave very similarly (even though the methods of proof are completely different). Secondly, it adds further evidence to what might be called a piece of folk knowledge in the field of quantum information theory: namely that stabilizer states are the natural finite-dimensional analogue of Gaussian states.

The paper is organized as follows. We survey previous work on the subject in Section 4.1.2. Section 4.2 is devoted to a superficial, yet self-contained introduction to Weyl operators, characteristic functions, Wigner distributions and stabilizer states. The main theorem is proven in Section 4.3. Sections 4.5 to 4.7 address various related topics. The results of these last three sections do not rely on each other. Concretely, we comment on the relation between stabilizer states and Gaussian states in Section 4.4; we consider mixed states with positive Wigner functions in Section 4.5 and use Section 4.7 for a discussion of Hilbert spaces whose dimension is the power of a prime.

Readers interested only in the structure of the proof, but not in its full generality, are deferred to Ref. [3], where a particularly simple special case of the main result is laid out.

4.1.2 Previous Results

Recently, Galvao *et. al.* took a first step into the direction of classifying the quantum states with positive Wigner function [38]. To explain the relationship of their results to the present paper, we have to comment on an axiomatic approach to discrete Wigner

functions and, further, on stabilizer states in dimensions that are the power of a prime number.

In Ref. [39], Gibbons, Hoffmann, and Wootters listed a set of requirements which should be met by any definition of a discrete Wigner function W. Denoting the dimension of the Hilbert space by d, their axioms amount to

1. *(Phase space)* W is a linear mapping sending operators to functions on a $d \times d$ lattice, called the *phase space*.

2. *(Translational covariance)* The Wigner function is covariant under the action of the Weyl operators (in the sense of Theorem 41).

3. *(Marginal probabilities)* There exists a function $Q(\lambda)$ that assigns a pure quantum state to every line λ in phase space. If ψ is state vector, then the sum of its Wigner function along λ must be equal to the overlap $|\langle Q(\lambda)|\psi\rangle|^2$.

Let us call functions that fall into this class *generalized Wigner functions*. This term is justified, as the characterization does not specify a unique solution: for a d-dimensional Hilbert space, there exist d^{d+1} distinct generalized Wigner functions. Note also that the construction has been described only for the case where $d = p^n$ is the power of a prime, because only then the notion of a *line* in phase space has a well-defined meaning.

We turn to the second remark, concerning stabilizer states. Consider a composite system, built of n d-level particles. We are free to conceive it as a single d^n-dimensional object. The two points of view give rise to different definitions of stabilizer states, the 'single-particle' one being starkly reduced as compared to the multiple-particle one. In Section 4.7, we show that the set of single-particle stabilizer states is strictly contained in the set of multi-particle ones. Indeed, the ratio of the respective cardinalities of the two sets grows super-exponentially in n. As an example, the generalized Bell and GHZ states

$$d^{-n/2} \sum_i |i\rangle \otimes |i\rangle, \qquad d^{-n/2} \sum_i |i\rangle \otimes |i\rangle \otimes |i\rangle,$$

arguably the best-known multi-particle stabilizer states, do not belong to the respective single-particle sets.

The result of Ref. [38] concerns quantum states in prime-power dimensions that are non-negative with respect to *all* possible definitions of generalized Wigner functions.

These states are shown to be mixtures of single-particle stabilizer states, as described above. The authors aim to establish necessary requirements for quantum computational speedup. Indeed, if the Wigner function of a quantum computer is positive at all times, then it operates only with stabilizer states and hence offers no advantage over classical computers, by the Gottesman-Knill Theorem.

Thus for the case of non-qubit pure states, Theorem 36 implies the results of Ref. [38] and goes further in two essential ways. Firstly, it suffices to look at a single definition of the Wigner function, as opposed to $d^{n(d^n+1)}$ generalized ones. Secondly, quantum computation and the Gottesman-Knill Theorem are naturally set in the context of *multiple* particles. Our definition assigns positive Wigner functions to all multiple-particle stabilizer states, while Ref. [38] effectively relies on the single-particle definition [2]. On the other hand, our main theorem does not address qubits or mixed states, which Galvao *et. al.* do.

4.2 Phase Space Formalism

The term *phase space formalism* encompasses the ideas and tools in relation to the *Weyl representation*, to be defined shortly. We will give a concise introduction in this section. Many of the results presented can be found in the literature, but some, e.g. the Clifford covariance of the Wigner function in non-prime dimensions, seem to be new.

4.2.1 Weyl representation

We start by considering a d-dimensional quantum system, d odd. In its Hilbert space $\mathcal{H}$, we choose a basis $\{|0\rangle, \ldots, |d-1\rangle\}$, labeled by elements of $\mathbb{Z}_d$. Henceforth, $\mathbb{Z}_d$ will be referred to as the *configuration space* and abbreviated by Q.

The pivotal objects in the phase space formalism are the *Weyl operators* (also known as the *generalized Pauli operators*), as constructed below. Let $\chi(q) = e^{\frac{2\pi}{d}iq}$. The relations

$$\hat{x}(q)|x\rangle = |x+q\rangle, \qquad \hat{z}(p)|x\rangle = \chi(px)|x\rangle \tag{4.2}$$

[2] Up to equivalence under Clifford operations.

define the *shift* and *boost* operators respectively. The Weyl operators are given by

$$w(p,q) = \chi(-2^{-1}pq)\,\hat{z}(p)\hat{x}(q), \tag{4.3}$$

for $p, q, t \in Q$. The specific choice of phases will prove useful later on [3]. The set of Weyl operators is closed under multiplication, up to phase factors. Direct computation shows that the composition law is given by

$$\begin{aligned} & w(p,q)w(p',q') \\ = \;& \chi(2^{-1}\left[\begin{pmatrix} p \\ q \end{pmatrix}, \begin{pmatrix} p' \\ q' \end{pmatrix}\right])\, w(p+p', q+q'). \end{aligned} \tag{4.4}$$

The square brackets denote the standard *symplectic inner product* on $\mathbb{Z}_d^2$:

$$\left[\begin{pmatrix} p \\ q \end{pmatrix}, \begin{pmatrix} p' \\ q' \end{pmatrix}\right] := \begin{pmatrix} p \\ q \end{pmatrix}^T J \begin{pmatrix} p' \\ q' \end{pmatrix} \tag{4.5}$$

where

$$J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{4.6}$$

We write $w(v) = w(v_p, v_q)$ for elements $v = (v_p, v_q) \in \mathbb{Z}_d^2$. The space $V := Q \times Q$ with inner product given by Eq. (4.5) will be called *phase space* in the sequel, owing to its analogy to the phase space known in classical mechanics.

The preceding constructing generalizes naturally to multiple particles. Indeed, the configuration space of an n-particle system is given by $Q = \mathbb{Z}_d^n$. Multiplication between two elements $p, q \in Q$ is understood as the usual inner product $pq = \sum_i p_i q_i$. The Hilbert space is again spanned by $\{|q\rangle\}_{q\in Q}$ and the Weyl operators are defined to be the

[3] The choice of phase factors ensures that the symplectic inner product Eq. (4.5) appears in the composition law Eq. (4.4) thus making the connection between the Weyl operators and symplectic geometry manifest. Other definitions in use, e.g. $w(p,q) = \hat{z}(p)\hat{x}(q)$ carry the same dependence in a less obvious manner. See also Refs. [36, 117].

tensor products

$$\begin{aligned} w(p,q) &= w(p_1,\ldots,p_n,q_1,\ldots,q_n) \\ &= w(p_1,q_1)\otimes\cdots\otimes w(p_n,q_n). \end{aligned} \tag{4.7}$$

Equations (4.4), (4.5) remain valid in the multiple-particle setting, if we substitute the matrix J by its multi-dimensional version

$$J = \begin{pmatrix} 0_{n\times n} & \mathbb{1}_{n\times n} \\ -\mathbb{1}_{n\times n} & 0_{n\times n} \end{pmatrix}.$$

We end this section with some miscellaneous remarks.

A state vector $|\psi\rangle$ can be identified with a complex function on configuration space by setting $\psi(q) = \langle q|\psi\rangle$. We will use both representations interchangeably.

The continuous Weyl operators $w(p,q) = e^{i(p\hat{X}-q\hat{P})}$, $p,q \in \mathbb{R}$ fulfill exactly the same composition law as stated in Eq. (4.4), if χ is set to $\chi(q) = e^{iq}$ and the other symbols are interpreted in the obvious way. In fact, Eq. (4.4) is then equivalent to the fundamental *Weyl commutation relations* [36]. Having this analogy in mind, p and q will sometimes be called *momentum* and *position* coordinates respectively.

For future reference, note the two simple relations

$$\left(w(p,q)\psi\right)(x) = \chi(-2^{-1}pq+px)\psi(x-q), \tag{4.8}$$

$$\operatorname{tr} w(p,q) = d^n\,\delta_{p,0}\delta_{q,0}. \tag{4.9}$$

It remains yet to justify the name Weyl *representation*. For $v \in V, t \in \mathbb{Z}_d$, define $w(v,t) = \chi(t)w(v)$. Equation (4.4) takes on the form

$$w(v_1,t_1)w(v_2,t_2) = w(v_1+v_2, t_1+t_2+2^{-1}[v_1,v_2]).$$

The set $V\times\mathbb{Z}_d$, equipped with the above composition law is called the *Heisenberg group* $H(\mathbb{Z}_d^n)$, the Weyl matrices constituting a unitary representation of $H(\mathbb{Z}_d^n)$ [36]. This point of view on Weyl operators will be needed only in Appendix 4.8.1.

4.2.2 Clifford group

The Clifford group is the subset of the unitary operators that map Weyl operators to multiples of Weyl operators under conjugation:

$$Uw(v)U^\dagger = c(v)w(S(v)) \tag{4.10}$$

for some maps $c : V \to \mathbb{C}$ and $S : V \to V$ [40]. The structure of the Clifford group is described in the following theorem [4].

Before stating the theorem, we have to comment on a re-appearing issue: namely that things are more involved if d is not a prime number. For prime values of d, $\mathbb{Z}_d$ has the structure of a *finite algebraic field*, $\mathbb{Z}_d^n$ is a *finite vector space* and most of the intuitions we have about vector spaces continue to be true. Among the more severe deficiencies of the general case is the fact that not every element a of $\mathbb{Z}_d$ possesses a multiplicative inverse modulo d. But even if the analogue of a theorem about vector spaces holds for non-prime values of d, it is often difficult to find a proof in the literature. Appendices 4.8.3 and 4.8.4 contain a collection of statements of this kind. Less technically inclined readers will not loose much by skipping these sections.

For the sake of clarity of language, we call functions f on Q which fulfill $f(\lambda a+b) = \lambda f(a)+f(b)$ *linear*, disregarding the fact that Q might fail to be a linear space. Similarly, a subset S of Q that is closed under addition and multiplication by elements of $\mathbb{Z}_d$ is referred to as a *subspace*. We define a function S to be *symplectic* if it is linear and preserves the symplectic form: $[S\,\cdot\,, S\,\cdot\,] = [\,\cdot\,,\,\cdot\,]$.

[4] Note that the "Clifford group" which appears in the context of quantum information theory [40] has no connection to the group by the same name used e.g. in the representation theory of $SO(n)$.

Theorem 37. (Structure of the Clifford group)

1. *For any symplectic S, there is a unitary operator $\mu(S)$ such that*

$$\mu(S)\, w(v)\, \mu(S)^\dagger = w(S\, v).$$

2. *μ is a* projective representation *of the symplectic group, that is*

$$\mu(S)\mu(T) = e^{i\phi}\mu(ST)$$

   for some phase factor $e^{i\phi}$.

3. *Up to a phase, any Clifford operation is of the form*

$$U = w(a)\mu(S)$$

   for a suitable $a \in V$ and symplectic S.

The representation μ is called the *Weil* or *metaplectic* representation [36, 123]. Theorem 37 is could be called a discrete version of the celebrated *Stone-von Neumann Theorem* [36]. Its proof is not essential for understanding the further argument and has therefore been moved to Appendix 4.8.1.

Note that a Clifford operation is connected to a vector a and a linear mapping S. This should remind us of a well-known structure on linear spaces: *affine transformations*. An affine mapping A is of the form $A(b) = S\, b + a$ where S is an invertible linear operator and a a vector. Let us call A symplectic if its linear part S is.

We will frequently use the 'dot notation' to define functions of one parameter; for example writing $S \cdot + a$ for A.

Lemma 38. (Clifford group and affine transformations) *The mapping*

$$S \cdot + a \mapsto w(a)\mu(S)$$

is a projective representation of the group of symplectic affine transformations.

Proof. All we need to do is to compare the composition law of the affine group

$$\begin{aligned}(S\cdot+a)\circ(T\cdot+b) &= S(T\cdot+b)+a\\ &= ST\cdot+(Sb+a)\end{aligned}$$

to the composition law of the representation

$$\begin{aligned}w(a)\mu(S)\;w(b)\mu(T) &= w(a)\;\mu(S)w(b)\mu(S)^\dagger\;\mu(S)\mu(T)\\ &= w(a)w(Sb)\mu(S)\mu(T)\\ &\propto w(Sb+a)\mu(S\,T)\end{aligned}$$

which proves the assertion. □

The correspondence established by the last lemma will find a very tangible manifestation in Section 4.2.4, when we will see that the Clifford group induces affine transformations of the Wigner function.

4.2.3 Fourier Transforms

Let $Q=\mathbb{Z}_d^n$ and $f:Q\to\mathbb{C}$ be a complex function on Q. The Fourier transform of f is

$$(\mathcal{F}f)(p)=\hat{f}(p) \;=\; |Q|^{-1/2}\sum_{q\in Q}\bar{\chi}(pq)f(q). \tag{4.11}$$

In the course of the main proof we will be confronted with Fourier transforms of functions which are defined only on a subspace of Q. If d is prime, then any subspace of $Q=\mathbb{Z}_d^n$ is of the form $\mathbb{Z}_d^{n'}$, for some $n'\leq n$, so no new situation arises.

For non-prime dimensions, however, subspaces may not be as well-behaved. Consider as an example $\{0,3,6\}\subset\mathbb{Z}_9^1$. The set is closed under addition and multiplication, but can clearly not be written as $\mathbb{Z}_9^{n'}$.

To cope with this problem, we will cast Eq. (4.11) into a form that is well-defined for functions f on more general spaces. The construction is presented below. It can be found in any textbook on harmonic analysis (e.g. Ref. [92]).

A *character* of Q is a function $\zeta:Q\to\mathbb{C}$ such that $\zeta(a+b)=\zeta(a)\zeta(b)$. Any

character of Q is of the form $\zeta(q) = \bar{\chi}(xq)$ for an appropriate $x \in Q$ (see Appendix 4.8.3). We can hence conceive the Fourier transformation defined in Eq. (4.11) as a function of the characters of Q:

$$\hat{f}(\zeta) = |Q|^{-1/2} \sum_q \zeta(q) f(q). \tag{4.12}$$

We denote the set of characters of Q by Q^*. With these notions, Eq. (4.12) defines a function $Q^* \to \mathbb{C}$. If, now, S is any subspace of Q and f a function on S, the Fourier transform

$$\hat{f} : S^* \to S \qquad \hat{f}(\zeta) = |S|^{-1/2} \sum_s \zeta(s) f(s)$$

is well-defined.

For $f : V \to \mathbb{C}$, we define the *symplectic Fourier transform* as

$$(\mathcal{F}_S f)(a) = |V|^{-1/2} \sum_{b \in V} \bar{\chi}([a,b]) f(b). \tag{4.13}$$

Finally, take a note that the normalization in Eqs. (4.11) and (4.12) has been chosen in such a way that *Parzeval's Theorem* $||f|| = ||\hat{f}||$ holds, where $||f||^2 = \sum_q |f(q)|^2$.

4.2.4 Definition and properties of the Wigner function

Employing Eq. (4.9) in conjunction with the composition law Eq. (4.4), one finds that the Weyl operators $\{w(p,q)\}$ form an orthonormal basis in the space of operators on $\mathcal{H}$ with respect to the trace scalar product $d^{-n}\ \mathrm{tr}(\,\cdot^\dagger\,\cdot\,)$. The *characteristic function* Ξ_ρ of an operator ρ is given by its expansion coefficients with respect to the Weyl basis:

$$\Xi_\rho(\xi, x) = d^{-n}\ \mathrm{tr}(w(\xi,x)^\dagger \rho). \tag{4.14}$$

We mentioned in the introduction that the continuous Wigner function is the symplectic Fourier transform of the characteristic function [36, 119]. The two latter concepts have been defined for finite-dimensional systems in the preceding paragraphs. We can now state, in complete analogy to the continuous case:

Definition 39. (Wigner function) *Let d be odd, $Q = \mathbb{Z}_d^n$ for some n. Let $V, \mathcal{H}$ be as usual and let ρ be a quantum state on $\mathcal{H}$.*

The Wigner function W_ρ *associated with ρ is the symplectic Fourier transformation of the characteristic function Ξ_ρ.*

An explicit calculation yields, for all $a \in V$,

$$\begin{aligned}(\mathcal{F}_S\,\Xi_\rho)\,(a) &= d^{-2n}\sum_{b\in V}\bar{\chi}([a,b])\,\mathrm{tr}(w(b)^\dagger\rho)\\ &= d^{-n}\,\mathrm{tr}(\left(d^{-n}\sum_b \bar{\chi}([a,b])w(b)^\dagger\right)\rho)\\ &=: d^{-n}\,\mathrm{tr}(A(a)\rho),\end{aligned} \tag{4.15}$$

where we have implicitly defined the *phase space point operator* $A(a)$ [39].

Theorem 40 lists a selection of properties of the Wigner function. For a more thorough discussion, the reader is deferred to Refs. [46, 117].

Theorem 40. (Properties of the Wigner function)

1. *The phase space point operators have unit trace and form an orthonormal basis in the space of Hermitian operators on $\mathcal{H}$. Hence the Wigner function of an Hermitian operator is real, and further, the* overlap

$$d^{-n}\ \mathrm{tr}(\rho\sigma) = \sum_{v\in V} W_\rho(v)W_\sigma(v),$$

and normalization *relations*

$$\sum_v W_\rho(v) = \mathrm{tr}\,\rho$$

hold.

2. *For a pure state ψ, the Wigner function $W_\psi := W_{|\psi\rangle\langle\psi|}$ equals*

$$\begin{aligned}&W_\psi(p,q) =\\ &d^{-n}\sum_{\xi\in Q}\bar{\chi}(\xi p)\bar{\psi}(q-2^{-1}\xi)\psi(q+2^{-1}\xi).\end{aligned}$$

3. *When computing marginal probabilities, the Wigner function behaves like a classical probability distribution:*

$$\sum_{p \in Q} W_\psi(p,q) = |\psi(q)|^2.$$

4. *The multi-particle phase space point operators factor:*

$$A(p_1,\ldots,p_n,q_1,\ldots,q_n) = \bigotimes_i^n A^{(i)}(p_i,q_i)$$

(and hence so does the Wigner function).

5. *It holds that* $A(0)|q\rangle = |-q\rangle$*. In other words, the phase space point operator at the origin equals the* parity operator.

6. *The Wigner function* $W_{\rho\,\sigma}$ *of an operator product is given by the* $\star$-product *(also known as the* Groenewold *or* Moyal product *[45]):*

$$\begin{aligned} & W_{\rho\,\sigma}(u) = (W_\rho \star W_\sigma)(u) \\ := \;& d^{-n} \sum_{v,w} W_\rho(u+v)\, W_\sigma(u+w) \bar{\chi}([v,w]). \end{aligned}$$

Proof. The proofs are all straight-forward; we give only hints on how to conduct them. It will be essential to recall the well-known relation

$$\sum_{x \in \mathbb{Z}_d^n} \chi(xy) = d^n\, \delta_{y,0}, \tag{4.16}$$

for all $y \in \mathbb{Z}_d^n$.

Indeed, the first claim can be proven by using Eq. (4.16) together with the definition of the phase space point operators Eq. (4.15). Employ Definition 39 and Eq. (4.16) to establish the second assertion, which in turn implies the third one. Theorem 40.4 makes use of the fact that $\bar{\chi}(pq) = \prod_i \bar{\chi}(p_i q_i)$; see also Section 4.7 for a very similar and more explicit calculation. The validity of the fifth statement is best shown using Eqs. (4.8), (4.16).

Let us lastly turn to Claim 6. We have noted that the phase space point operators form an orthonormal system. Hence we can expand an operator ρ in terms of its Wigner function as $\rho = \sum_v W_\rho(v)A(v)$. Substituting ρ and σ by their respective expansions in $W_{\rho\sigma}(v) = d^{-n}\operatorname{tr}(A(v)\rho\sigma)$ yields the desired formula with the help of Lemma 63. □

The following statement will be vital to the proof of the main theorem. It assigns an elegant geometric interpretation to the Clifford group.

Theorem 41. (Clifford Covariance) *Let $U = w(a)\mu(S)$ be a Clifford operation. Let $\rho' := U\rho U^\dagger$ for some Hermitian operator ρ. The Wigner function is* covariant *in the sense that*

$$W_\rho(v) = W_{\rho'}(S\,v + a).$$

Proof. We compute the action of the Clifford group on the phase space point operators.

$$\begin{aligned}
& w(a)\mu(S)\,A(b)\,\mu(S)^\dagger w(a)^\dagger \\
= \;& d^{-n}\sum_{v\in V}\bar\chi([b,v])w(a)\mu(S)\,w(v)\,\mu(S)^\dagger w(a)^\dagger \\
= \;& d^{-n}\sum_{v}\bar\chi([b,v])w(a)\,w(S\,v)\,w(a)^\dagger \\
= \;& d^{-n}\sum_{v}\bar\chi([b,v])\chi([a,S\,v])w(S\,v) \\
= \;& d^{-n}\sum_{v':=S\,v}\bar\chi([b,S^{-1}v'])\bar\chi([a,v'])w(v') \\
= \;& d^{-n}\sum_{v'}\bar\chi([S\,b+a,v'])w(v') = A(Sb+a).
\end{aligned}$$

The claim follows by use of Eq. (4.15). □

Our definition of the discrete Wigner function coincides with the ones used in Refs. [46, 116, 117, 126]. It is further equal to Leonhardt's version [74], up to a permutation of points in phase space; it corresponds to choice (a) in Ref. [71] and lastly to $G = \mathbb{Z}_d^n$ in Ref. [24]. One can show that W, as defined here, fulfills the axioms of Ref. [39] which had been laid out in Section 4.1.2. Put differently, it is an element of the set of generalized Wigner functions. Gibbons *et. al.* remarked in Ref. [39] that among the generalized Wigner functions, some stand out by their high degree of symmetry. In our language, this symmetry is an incarnation of the Clifford covariance established

in Theorem 41. Naturally, it is now interesting to ask how much freedom is left in the definition of a Wigner function, once one requires Clifford covariance to hold. We show in Appendix 4.8.2 that the definition used here is virtually unique in that regard.

4.2.5 Stabilizer States

Using the composition law of the Heisenberg group Eq. (4.4), it is easy to see that two Weyl operators $w(v_1), w(v_2)$ commute if and only if $[v_1, v_2] = 0$. Now consider the image of an entire subspace M under the Weyl representation w. The set

$$w(M) = \{w(m) | m \in M\}$$

consists of mutually commuting operators if and only if the symplectic form vanishes on M:

$$[m_1, m_2] = 0, \quad \text{for all } m_i \in M.$$

Spaces of that kind are called *isotropic*. Clearly, if M is isotropic, then the operators $w(M)$ can be simultaneously diagonalized. We will see that if $|M| = d^n$, the eigenspaces become non-degenerate and can thus be used to single out state vectors in the Hilbert space. A subspace M of V is said to be *maximally isotropic* if its cardinality equals d^n. See Appendix 4.8.3 for a justification of that nomenclature.

Lemma 42. (Stabilizer States) *Let M be a maximally isotropic subspace of V. Let $v \in V$. Up to a global phase, there is a unique state vector $|M, v\rangle$ that fulfills the eigenvalue equations*

$$\chi([v, m]) w(m) \, |M, v\rangle = |M, v\rangle$$

for all $m \in M$.

Proof. Existence: It is elementary to check that

$$|M|^{-1} \sum_{m \in M} \chi([v, m]) w(m) \tag{4.17}$$

is a rank one projection operator fulfilling the eigenvalue equations.

Uniqueness: According to Appendix 4.8.3, there are p^n characters of M, each giving rise to a distinct projection operator as defined in the last paragraph. Two distinct operators of that kind are mutually orthogonal, because they belong to different eigenvalues of at least one of the Weyl operators. But $\dim \mathcal{H} = |Q| = p^n$ and thus there is no space for more than one-dimensional solutions to the given set of equations. □

The state vector $|M, v\rangle$ is called the *stabilizer state* associated to M and v. For obvious reasons, one refers to the set of operators $\{\chi([v, m])\, w(m) | m \in M\}$ as the *stabilizer* of $|M, v\rangle$. Due to the isotropicity of M, the stabilizer is closed under multiplication and thus constitutes a group. Occasionally, we write $|M\rangle$ for $|M, 0\rangle$. To specify a stabilizer state, we need to specify a maximally isotropic space M. This is best done by giving a basis $\{m_1, \ldots, m_k\}$ of M. It is convenient to assemble the basis vectors as the columns of a $2n \times k$-matrix, which is generally referred to as the *generator matrix*. As the choice of a basis is non-unique, so is the form of the generator matrix.

A stabilizer state $|M\rangle$ is a *graph state* if it possesses a generator matrix of the form

$$\begin{pmatrix} \vartheta \\ \mathbb{1}_{n\times n} \end{pmatrix}, \tag{4.18}$$

where ϑ is a symmetric $n \times n$-matrix [55]. The designation stems from the fact that ϑ can be interpreted as the adjacency matrix of a graph. Many properties of $|M\rangle$ are describable in terms of that graph alone [55]. Some authors require the diagonal elements ${\vartheta^i}_i$ to vanish (equivalently, no vertex of the graph should be linked to itself), but we will not impose that restriction. Note that there exist considerably more general definitions of graph states [96].

Obviously, we will be concerned with Wigner functions of stabilizer states. Lemma 43 clarifies their structure.

Lemma 43. (Wigner functions of stabilizer states) *The Wigner function of a stabilizer state* $|M, v\rangle$ *is the* indicator function *on* $M + v$. *More precisely,*

$$W_{|M,v\rangle}(a) = \frac{1}{d^n}\delta_{M+v}(a) = \frac{1}{d^n}\begin{cases} 1 & a \in M + v \\ 0 & \text{else.} \end{cases}$$

Proof. The representation given in Eq. (4.17) of $|M, v\rangle$ determines the characteristic function

$$\Xi_{|M,v\rangle}(b) = d^{-n}\,\chi([v,b])\delta_M(b).$$

We compute the symplectic Fourier transformation:

$$\begin{aligned}\big(\mathcal{F}_S\,\Xi_{|M,v\rangle}\big)(a) &= d^{-2n}\sum_{b\in V}\bar{\chi}([a,b])\chi([v,b])\delta_M(b)\\ &= d^{-2n}\sum_{b\in M}\bar{\chi}([a-v,b])\\ &= d^{-n}\,\delta_{M^\perp}(a-v).\end{aligned}$$

Where

$$M^\perp = \{v \in V | [m,v] = 0 \text{ for all } m \in M\}$$

is the *symplectic complement* of M in V. But M is a maximally isotropic space and hence $M = M^\perp$ (see Appendix 4.8.3). □

In particular we know now that the Wigner function of stabilizer states is non-negative. The next sections are devoted to the proof of the converse.

4.3 Discrete Hudson's Theorem

4.3.1 Bochner's Theorem

Define the *self correlation function*

$$K_\psi(q,x) = \psi(q + 2^{-1}x)\bar{\psi}(q - 2^{-1}x)$$

and note that the Wigner function fulfills

$$W(p,q) = \frac{1}{d^n}\sum_{x\in Q}\bar{\chi}(px)K_\psi(q,x). \tag{4.19}$$

Fix a $q_0 \in Q$. Designating the function $p \mapsto W(p,q_0)$ by $W(\,\cdot\,,q_0)$, Eq. (4.19) says that $W(\,\cdot\,,q_0)$ is the Fourier transform of $K(q_0,\,\cdot\,)$. Therefore, W is non-negative if and

only if the d^n functions $K(q_0, \cdot\,)$ have non-negative Fourier transforms.

In harmonic analysis, the set of functions with non-negative Fourier transforms is characterized via a theorem due to Bochner. It is usually proven either in the context of Fourier analysis on the real line or else, in full generality, for harmonic analysis on – not necessarily abelian – locally compact groups. While the former statement is not general enough for our purpose, the latter is not easily accessible. However, it turns out that in the discrete abelian setting an elementary proof can be given. It is stated in the next theorem, along with a variation for subsequent use.

Theorem 44. (Variations of Bochner's Theorem) *Let M be a subspace of Q. Let $f : M \to \mathbb{C}$. It holds that*

1. *The Fourier transform of f is non-negative if and only if the matrix*

$$A^x{}_q = f(x-q) \qquad (x, q \in M)$$

   is positive semi-definite.

2. *The Fourier transform of f has constant modulus (i.e. $|\hat{f}(x)| = \mathrm{const}$) if and only if f is orthogonal to its translations:*

$$\langle f, \hat{x}(q) f \rangle = \sum_{x \in M} \bar{f}(x) f(x-q) = 0$$

   for all non-zero $q \in M$.

Proof. The following computation is a variant of a well-known fact concerning circulant matrices. We claim that any character ζ of M is an eigenvector of A with eigenvalue $\lambda = |M|^{-1/2}\, \hat{f}(\zeta)$. Indeed, plugging in the definitions yields

$$\begin{aligned}
(A\,\zeta)(x) &= \sum_q A^x{}_q\, \zeta(q) \\
&= \sum_q f(x-q)\zeta(q) \\
&= \sum_q f(q)\bar{\zeta}(q)\, \zeta(x) \\
&= \sqrt{|M|}\hat{f}(\zeta)\, \zeta(x).
\end{aligned}$$

There exist $|M|$ characters and thus equally many eigenvectors of A. Therefore, A can diagonalized. All its eigenvalues are non-negative if and only if $\hat{f}$ is non-negative.

By the same argument, A is proportional to a unitary matrix if and only if $|\hat{f}(q)|$ is constant. But a matrix is unitary if and only if its rows form an ortho-normal set of vectors. □

From here, the proof proceeds in two steps. Section 4.3.2 harvests Theorem 44.1 to gain information on the pointwise modulus $|\psi(q)|$ of a vector with non-negative Wigner function. Building on these finding, we will analyze the properties of such Wigner functions in Section 4.3.3.

4.3.2 Supports and Moduli

Lemma 45. (Modulus Inequality) *Let ψ be a state vector with non-negative Wigner function.*

It holds that

$$|\psi(q)|^2 \geq |\psi(q-x)|\,|\psi(q+x)|$$

for all $q, x \in Q$.

Proof. Fix a $q \in Q$. As W_ψ is non-negative, so is the Fourier transform of $K_\psi(q, \cdot)$. Bochner's Theorem implies that the matrix ${A^x}_y = K(x-y, q)$ is positive semi-definite which in turn implies that all principal sub-matrices are psd. In particular the determinant of the 2×2 principal sub-matrix

$$\begin{aligned} &\begin{pmatrix} K_\psi(q,0) & K_\psi(q,2x) \\ K_\psi(q,-2x) & K_\psi(q,0) \end{pmatrix} \\ = &\begin{pmatrix} |\psi(q)|^2 & \psi(q+x)\bar{\psi}(q-x) \\ \bar{\psi}(q+x)\psi(q-x) & |\psi(q)|^2 \end{pmatrix} \end{aligned}$$

must be non-negative. But this means

$$|\psi(q)|^4 - |\bar{\psi}(q+x)\psi(q-x)|^2 \geq 0,$$

which proves the theorem. □

We will call the set $\operatorname{supp}\psi$ of points where a state-vector is non-zero its *support*. $S = \operatorname{supp}\psi$ has the property to contain the *midpoint* of any two of its elements. Indeed, if $a, b \in S$, then setting $q = 2^{-1}(a+b)$ and $x = 2^{-1}(a-b)$ in the Modulus Inequality shows that

$$|\psi(2^{-1}(a+b))| \geq |\psi(a)|\,|\psi(b)| > 0,$$

hence $2^{-1}(a+b) \in S$. Let us refer to sets possessing this quality as being *balanced*.

The following lemma clarifies the structure of balanced sets. Recall that a subset A of V is *affine* if $A = M + v$ for a subspace M and some vector v. An affine space is a subspace if and only if it contains the origin 0.

Lemma 46. (Balanced sets) *A subset S of Q is balanced if and only if S is an affine space.*

Proof. We show the 'only if' part, the other one being simple.

As both the characterizations of balancedness and affinity are invariant under translation, there is no loss of generality in assuming that $0 \in S$. We have to establish that S is closed under both addition and scalar multiplication.

Let $a \in S$. We claim that

$$2^{-l}\lambda\, a \in S \tag{4.20}$$

for all $l \in \mathbb{N}$ and $\lambda \leq 2^l$. The proof is by induction on l. Suppose Eq. (4.20) holds for some l. If $\lambda \leq 2^{l+1}$ is even, then $2^{-l-1}\lambda\, a = 2^{-l}(\lambda/2)b \in S$. Else,

$$2^{-l-1}\lambda\, a = 2^{-1}\big(2^{-l}\frac{\lambda-1}{2}\, a + 2^{-l}\frac{\lambda+1}{2}\, a\big) \in S,$$

which shows the validity of Eq. (4.20).

There exists an integer $l > d$ such that $2^l = 1 \mod d$. Indeed, by Euler's Theorem, $2^{\phi(d)} = 1 \mod d$, where ϕ is Euler's totient function. So $l = d\phi(d)$ satisfies the requirements. Inserting l into Eq. (4.20), we conclude that $\lambda\, a \in S$ for all $\lambda \leq 2^d$. Thus certainly $\lambda\, a \in S$ for all $\lambda \in \mathbb{Z}_d$ and we have proved closure under scalar multiplication.

If $a, b \in S$ then, by the last paragraph $2a, 2b \in S$ and hence $2^{-1}(2a+2b) \in S$, establishing closure of S under addition. □

Lemma 47. (Constant Modulus) *Let ψ be a state vector with non-negative Wigner function. Then $|\psi(\,\cdot\,)|$ is constant on the support of ψ.*

Proof. Pick two points $x, q \in \operatorname{supp}\psi$ and suppose $|\psi(q)| > |\psi(x)|$.

Letting $z = x - q$, the assumption reads $|\psi(q)| > |\psi(q+z)|$. The Modulus Inequality, centered at $q + z$, gives

$$|\psi(q+z)|^2 \;\geq\; |\psi(q)|\,|\psi(q+2z)|. \tag{4.21}$$

As $\operatorname{supp}\psi$ is affine, we know that $\psi(q + kz) \neq 0$ for all $k \in \mathbb{Z}_d$. Hence Eq. (4.21), together with the assumption implies

$$\begin{aligned} & |\psi(q+z)|^2 > |\psi(q+z)|\,|\psi(q+2z)| \\ \Leftrightarrow\;\; & |\psi(q+z)| > |\psi(q+2z)|. \end{aligned}$$

By inducting on this scheme, we arrive at

$$|\psi(q)| > |\psi(q+z)| > |\psi(q+2z)| > \cdots$$

and therefore $|\psi(q)| > |\psi(q+dz)| = |\psi(q)|$, which is a contradiction.

Thus $|\psi(q)| \leq |\psi(x)|$. Swapping the roles of x and q proves that equality must hold. □

At this point, we have full knowledge of the pointwise *modulus* of a state vector with non-negative Wigner function. The *phases* of $\psi(\,\cdot\,)$ are, however, completely unknown. The section to come addresses this problem indirectly, by studying non-negative Wigner functions.

4.3.3 Non-negative Wigner functions

To motivate the following, assume for a moment that ψ has a non-negative Wigner function and further, that $\psi(q) \neq 0$ for all q. Choose a $q_0 \in Q$ and consider the function $W(\,\cdot\,, q_0)$. Lemma 47 implies that $K_\psi(q_0, \,\cdot\,)$ has constant modulus and hence – by Theorem 44.2 – $W(\,\cdot\,, q_0)$ must be orthogonal to its translations. Clearly, a non-negative

function possesses this property if and only if it is supported on at most a single point.

There hence exists a $p_0 \in Q$ such that $W(p, q_0) \propto \delta_{p,p_0}$. This observation starkly reduces the possible forms of positive Wigner functions; it will be generalized to state vectors with arbitrary support in the next lemma.

Lemma 48. *Let ψ be a state vector. If W_ψ is non-negative, then it is of the form*

$$W_\psi(v) = d^{-n}\, \delta_T(v)$$

where $T \subset V$ is a set of cardinality d^n.

What is more, if $0 \in T$, then the set of elements of T with vanishing position coordinates

$$\{(p, 0) \in T \,|\, p \in Q\}$$

is a subspace of V.

Proof. Let $S = \operatorname{supp} \psi$. Again, we may assume that S is a subspace of Q, for else we replace ψ by $w(-s)\psi$ for some $s \in S$. It follows that $\operatorname{supp} K_\psi = S \times S$. Indeed,

$$\begin{aligned} K_\psi(q, x) \neq 0 \quad &\Leftrightarrow \quad q \pm 2^{-1}x \in S \\ &\Leftrightarrow \quad q \in S \wedge x \in S. \end{aligned}$$

Denote by $S^\perp = \{q \in Q | sq = 0 \text{ for all } s \in S\}$ the orthogonal complement of S [5]. We will adopt the common notation $[p] = p + S^\perp$ for cosets of $S^\perp$. It should be clear that $[p]$ is nothing other but the *affine space* with directional vector space given by $S^\perp$ and base vector p. The set S^* of characters of S can be identified with $Q/S^\perp$. Certainly, $s \mapsto \chi(ps)$ defines a character of S for every $p \in Q$. Further, $\chi(ps) = \chi(p's)$ for all $s \in S$ if and only if $p - p' \in S^\perp$. That indeed all elements of S^* can be obtained this way is shown in Corollary 60.

Define K'_ψ to be the restriction of K_ψ to its support $S \times S$. For the rest of the proof,

[5] For subsets S of Q, $S^\perp$ denotes the *orthogonal* complement, while for subsets S of V the same symbol refers to the *symplectic* complement. This notation is natural, as for both Q and V only one respective inner product has been defined.

we fix a $q_0 \in S$. Now consider

$$\begin{aligned} W(p,q_0) &= d^{-n} \sum_{x \in Q} \bar{\chi}(px) K(q_0,x) \\ &= d^{-n} \sum_{x \in S} \bar{\chi}(px) K'(q_0,x). \end{aligned}$$

Viewed as a function in p, $W(p,q_0)$ has constant values on cosets of $S^\perp$. Therefore,

$$W'([p],q) := d^n |S|^{-1/2} W(p,q) \tag{4.22}$$

is a well-defined function on S^*. The considerations of the previous paragraph allow us to identify $W'([\,\cdot\,],q_0)$ as the Fourier transform of $K'(q_0,\cdot)$.

We can now repeat the argumentation presented just before the current lemma. Indeed, the modulus of $K'(q_0,[\,\cdot\,])$ is constant and W' is non-negative. Furthermore, by definition of q_0, $K'(q_0,[\,\cdot\,])$ is non-zero and we may thus conclude that $p \mapsto W'([p],q_0)$ is supported on exactly one coset $[p_0]$.

Normalization of ψ implies $|\psi(\,\cdot\,)| = |S|^{-1/2}$. Hence $|K'_\psi(q_0,\,\cdot\,)| = |S|^{-1}$ and

$$||K'_\psi(q_0,\,\cdot\,)||^2 = \sum_x |K'_\psi(q_0,x)|^2 = |S|^{-1}.$$

By Parzeval's Theorem, $||W'([\,\cdot\,],q_0)||^2 = |S|^{-1}$ as well. It follows that $W'([p_0],q_0) = |S|^{-1/2}$.

Inverting Eq. (4.22) gives

$$W(p,q) = d^{-n} \begin{cases} 1 & [p] = [p_0] \\ 0 & \text{else} \end{cases} \tag{4.23}$$

which proves the first claim of the lemma. The cardinality of T is fixed by the normalization of the Wigner function (Theorem 40.40).

Now suppose $W(0,0) = W'([0],0) \neq 0$. Clearly, then $W(p,0)$ is non-zero if and only if $p \in [0] \Leftrightarrow p \in S^\perp$. The last assertion of the lemma follows, since $S^\perp$ is a subspace of Q. □

So a non-negative Wigner function is the indicator functions of some set T. This

finding is compatible with Lemma 43, which describes the structure of Wigner functions of stabilizer states. The next two lemmas verify that T has indeed all the properties of the sets that appear in Lemma 43.

Lemma 49. *Let ψ be a state vector. If W_ψ is of the form*

$$W_\psi(v) = d^{-n}\,\delta_T(v),$$

then T is an affine space.

Proof. The proof proceeds similar to the one of Lemma 46. There is no loss of generality in assuming that $0 \in T$.

First, we show that T is closed under scalar multiplication. To this end, pick a point $a \in T$. There exists a symplectic mapping S that sends a to a vector a' of the form $(a'_p, 0)$ where $a'_p \in Q$ (see Appendix 4.8.4). The set $T' = S\,T$ is the support of the Wigner function of $\mu(S)\psi$. By the second assertion of Lemma 48, $\lambda a' \in S\,T$ for every $\lambda \in \mathbb{Z}_d$. Hence $S^{-1}(\lambda a') = \lambda a \in T$.

Turning to closedness under addition, let $a, b \in T$. By the last paragraph, $2a, 2b \in T$. Arguing as before, note that the set $T - 2a$ is the support of the Wigner function of $w(-2a)\psi$ and thus closed under multiplication. As $2b - 2a \in T - 2a$, we know that $b - a \in T - 2a$ and hence $b + a \in T$. □

Lemma 50. *Let ψ be a state vector such that W_ψ is of the form*

$$W_\psi(v) = d^{-n}\delta_T(v).$$

If T is a subspace, then it is isotropic.

Proof. The vector ψ describes a pure state, hence $W_\psi \star W_\psi = W_\psi$ (recall the Moyal product, introduced in Theorem 40). Let $u \in T$. Plugging in the definitions gives

$$\begin{aligned} & W_\psi \star W_\psi(u) \\ = \quad & d^{-n} \sum_{v,w \in V} W_\psi(u+v)\, W_\psi(u+w) \bar{\chi}([v,w]) \\ = \quad & d^{-3n} \sum_{v,w \in T} \bar{\chi}([v,w]). \end{aligned}$$

Note that $\sum_{w \in T} \bar{\chi}([v,w]) \leq |T| = d^n$ with equality if and only if $[v,w] = 0$ for all w. Hence

$$W_\psi \star W_\psi(u) \leq d^{-n} = W_\psi(u).$$

For the left-hand and the right-hand side to be equal, T must be isotropic. □

Therefore T, as defined above, is of the form $T = M + v$ where M is an isotropic space of cardinality d^n. But then, W_ψ is the Wigner function of a stabilizer state, by Lemma 43. We have proven:

Theorem 51. (Main Theorem) *Let $\psi \in L^2(\mathbb{Z}_d^n)$ be a state vector. If the Wigner function of ψ is non-negative, then ψ is a stabilizer state.*

4.4 Discrete Gaussians

It has long been realized that the coefficients of stabilizer state vectors are described by quadratic forms. However, the current literature either neglects the non-prime case (Refs. [30, 42, 96]) or is less explicit (Ref. [59]) than the following lemma in showing the tight relation between Gaussian states and stabilizer states.

We will concentrate on stabilizer states with full support. This constitutes only a modest restriction of generality. Indeed, let ψ be a general stabilizer state, let $Q' := \operatorname{supp} \psi$. Let us for the sake of simplicity assume that d is prime and Q' is a subspace of Q. The restriction of the coordinate function $\psi(q)$ to Q' can be thought of as defining a vector ψ' of a quantum state of an $n' := \dim Q'$ particle system. It is now possible to check that ψ' is a stabilizer state. In this way any stabilizer state can be viewed as one with full support, possibly on a smaller system. We will, however, not take the time to make this construction precise nor will we rely on it in this paper.

Lemma 52. *Let ψ be a state vector. The following statements are equivalent.*

1. *ψ is a stabilizer state and $\psi(q) \neq 0$ for all $q \in Q$.*
2. *Up to the action of a Weyl operator, ψ is a graph state.*

3. *There exists a symmetric $n \times n$-matrix θ and an $x \in Q$ such that*

$$\psi(q) = \omega^{q\theta q + xq}.$$

Proof. (1 ⇒ 2). By assumption $|\psi\rangle = |M, v\rangle$ for some maximal isotropic space M and a vector v. We claim that there is no non-zero $p \in Q$ such that $(p, 0) \in M$.

For suppose there exists such a p. Then

$$\langle q|w(p,0)|M\rangle = \chi(-pq)\langle q|M\rangle.$$

On the other hand,

$$\langle q|w(p,0)|M\rangle = \bar{\chi}([v,(p,0)])\,\langle q|M\rangle,$$

by the definition of $|M, v\rangle$. Hence $\operatorname{supp}|M\rangle$ must be contained within a hyper-surface of Q specified by $pq = \text{const}$, which contradicts the assumption that $\operatorname{supp}\psi = Q$.

There are d^n elements in M. By the last paragraph, no two of them have the same position coordinates. As there exist only $d^n = |Q|$ possible choices for the position coordinates, one can find for every $q \in Q$ a $p \in Q$ such that $(p, q) \in M$. Let $e_1, \ldots, e_n$ denote the canonical basis of $\mathbb{Z}_d^n$. Choose $m_1, \ldots, m_n \in M$ such that the position part of m_i equals e_i. The span of $\{m_i\}_{i=1,\ldots,n}$ has clearly cardinality d^n, so we have found a basis of M. By construction, the generator matrix composed of these basis vectors has the form shown in Eq. (4.18) with some $n \times n$-matrix θ. It is not hard to see that M is isotropic if and only if θ is symmetric, establishing that $|M\rangle$ is a graph state. Theorem 41 and Lemma 43 show that $w(v)|M\rangle = |M, v\rangle = |\psi\rangle$.

(2 ⇒ 3). Let M be an isotropic space which possesses a generator matrix of the form given in Eq. (4.18). Let $m_i = (\vartheta_i, e_i)$ be the ith column of that matrix. We need to establish the existence of a symmetric matrix θ and an $x \in Q$ such that

$$\langle q|M, v\rangle = \omega^{q\theta q + xq} =: \psi(q).$$

Indeed, choose

$$\theta = 2^{-1}\vartheta, \qquad x_i = [v, m_i].$$

Using Eq. (4.8), one can then check by direct computation that ψ fulfills the defining eigenvalue equations

$$\chi([v, m_i])w(m_i)\psi = \psi$$

and hence $|\psi\rangle = |M, v\rangle$, by Lemma 42.

(3 ⇒ 1). Reverting the previous proof shows that ψ is a graph state. It has maximal support by definition. □

The claimed analogy between stabilizer states and Gaussian states is apparent when comparing statement 3 to Theorem 35.

4.5 Mixed States

It is natural to ask how the results obtained before generalize to mixed states. Certainly, mixtures of stabilizer states are non-negative on phase space and it might be surmised that all such quantum states are convex combinations of stabilizer ones. In the context of continuous variable systems, Bröcker and Werner refuted an analogous conjecture by giving a counter-example [17]. Again, the situation is similar in the finite setting, as will be shown now.

As a consequence of Theorem 40.5, $A(0)$ can be decomposed as $A(0) = P_+ + P_-$, where $P_\pm$ denotes the projector onto the symmetric and antisymmetric state vectors respectively. Since $P_+ + P_- = \mathbb{1}$, we have that $P_- = 1/2(\mathbb{1} - A(0))$. Because we know the Wigner functions of both $\mathbb{1}$ ($W(v) = d^{-n}$) and of $A(0)$ ($W(v) = \delta_{v,0}$), we immediately obtain

$$W_{P_-}(v) = \frac{1}{2}\begin{cases} d^{-n} - 1 & v = 0 \\ d^{-n} & \text{else.} \end{cases} \tag{4.24}$$

For a single three-dimensional quantum system there exists a unique antisymmetric state vector $|\psi_-\rangle = 2^{-1/2}(|+1\rangle - |-1\rangle)$, hence $P_- = |\psi_-\rangle\langle\psi_-|$. Figure 4.2 depicts the Wigner function of the state ρ, obtained by mixing the pure states

$$|\psi_-\rangle, w(-1, 0)|\psi_-\rangle, w(-1, -1)|\psi_-\rangle$$

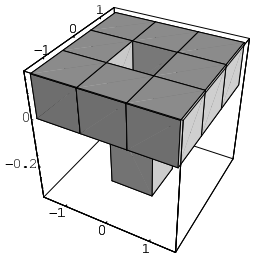


Figure 4.1: Wigner function of the antisymmetric vector $|\psi_-\rangle$.

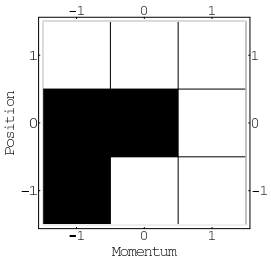


Figure 4.2: Wigner function of the equal mixture of the vectors $|\psi-\rangle, w(-1,0)|\psi_-\rangle$ and $w(-1,-1)|\psi_-\rangle$. White squares stand for a value of $1/6$, black squares for 0.

with equal weights.

The Wigner function of a single-particle stabilizer state is a line in the two-dimensional phase space, according to Lemma 43. There are $d(d+1)$ such lines and hence equally many stabilizer states. Assume these states have been brought into some order and denote the associated projection operators by $P_1, \ldots, P_{d(d+1)}$. Let $\rho = \sum_i^{d(d+1)} \lambda_i P_i$ be a convex decomposition of ρ in terms these operators. If there is a point v in phase space where $W_\rho(v) = 0$ and $W_{P_i}(v) \neq 0$, then clearly λ_i must vanish. By exhaustively listing all 12 lines in $\mathbb{Z}_3^2$, one finds that ρ can have non-zero coefficients only with respect to the stabilizer states whose Wigner functions are shown in Figure 4.3.

But ρ admits no convex decomposition in terms of these three lines. Indeed, no two of them cover all the points in the support of W_ρ, so only a mixture of all three lines could potentially suffice. Now notice that the point $(1,-1)$ is an element only of

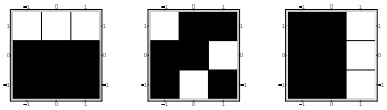


Figure 4.3: The white squares mark all lines in $\mathbb{Z}_3^2$ that do not intersect any point where the Wigner function shown in Fig. 4.2 vanishes.

the third line, while $(1, 0)$ is contained in both the second and the third one. Therefore any mixture of these three lines takes on a higher value on $(1, 0)$ than on $(1, -1)$. The distribution W_ρ, on the other hand, is constant on its support.

4.6 Dynamics

Having established which quantum states give rise to non-negative phase space distributions, the next step is to characterize the set of operations that preserve this property. We have seen in Section 4.2.4 that Clifford unitaries implement permutations in phase space and thus manifestly preserve positivity. They are unique in that regard, as will be shown now.

By the results of Section 4.3, it is apparent that a unitary operation U can preserve positivity only if it sends stabilizer states to stabilizer states. One can reasonably conjecture that only Clifford operations possess this feature and in the case of single-particles in prime-power dimensions, a proof of this fact has been given in Ref. [38]. The general case, however, poses surprising difficulties which have forced us to take a less direct route.

Let us shortly pause to clarify our objectives. We aim to characterize the set of unitaries U that satisfy statements of the kind: $W_{U\rho U^\dagger}$ is non-negative whenever W_ρ is. We can require the above statement to hold for *any* Hermitian operator ρ, or just whenever ρ is a *quantum state*. In the former case the restrictions on U are much stronger than in the latter one. Indeed, by considering the image of the phase space point operators $A(a)$ under the action of U and making use of Lemma 63, it is straight-forward to prove that only Clifford operations can preserve positivity of the Wigner functions of general Hermitian operators. The following theorem is slightly more ambitious in considering only the action of U on quantum states.

Theorem 53. (Only permutations preserve positivity). *Let U be unitary. If, for all quantum states ρ with non-negative Wigner function, it holds that $W_{U\rho U^\dagger}$ is non-negative, then U is Clifford.*

Proof. Firstly, take a note that substituting 'quantum state' by 'positive operator' in the above theorem, only amounts to a change of normalization and does not alter the

statement. Set

$$\begin{aligned}\mu(\rho) &:= \min_{v\in V} W_\rho(v),\\ \nu(\rho) &:= \operatorname{minarg} W_\rho := \{v \in V | W_\rho(v) = \mu(v)\}.\end{aligned}$$

Let ρ be such that $\mu(\rho) < 0$. We claim that $\mu(\rho) = \mu(\rho')$, where $\rho' = U\rho U^\dagger$. In other words: U preserves minimal values.

Indeed, there exists positive constants $\lambda_{1,2}$ such that

$$\lambda_1\mu(\rho') + \lambda_2 d^{-n} = 0.$$

Hence $\sigma := \lambda_1\rho + \lambda_2\mathbb{1}$ has a non-negative Wigner function. The assumption $\mu(\rho') < \mu(\rho)$ yields

$$W_{U\sigma U^\dagger}(v) = \lambda_1\mu(\rho') + \lambda_2 d^{-n} < 0$$

for every $v \in \nu(\rho')$, which contradicts the defining property of U. Thus $\mu(\rho') \leq \mu(\rho)$. Substituting U by U^{-1} shows that equality of $\mu(\rho)$ and $\mu(\rho')$ must hold.

Now set

$$\rho(a) := (1 - d^{-n})^{-1}\, w(a) P_-\, w(a)^\dagger$$

for all $a \in V$. We have $\mu(\rho(a)) = \mu(\rho'(a)) = -1$ and $\nu(\rho) = \{a\}$. The crucial observation lies in the fact that $\nu(\rho')$ contains only a single point as well. So, U preserves the 'pointed' shape of $W_\rho(a)$. To see why that is the case, suppose there is a a_0 such that $|\nu(\rho(a_0)')| > 1$. There are d^{2n} operators $\rho(a)'$ and equally many points in phase space, so there exists an a_1 such that $\nu(a_0)$ and $\nu(a_1)$ intersect in at least one point v. Define $\sigma = 1/2(\rho(a_0) + \rho(a_1))$. It holds that $\mu(\sigma) > -1/2$, whereas $W_{\sigma'}(v) = -1$ which is a contradiction. There is hence a well-defined function S which sends a to the unique element of $\nu(\rho(a)')$.

Finally, let σ be any density matrix. The idea is to mix σ very weakly to $\rho(a)$, so that the positions of the minima of the mixture are still determined by $\rho(a)$. Indeed, there

exists an $\epsilon > 0$ such that

$$\begin{aligned}
\nu(\rho(a) + \epsilon\sigma) &= \{a\} \\
\mu(\rho(a) + \epsilon\sigma) &= -1 + \epsilon\, W_\sigma(a); \\
\nu(\rho(a)' + \epsilon\sigma') &= \{S(a)\} \\
\mu(\rho(a)' + \epsilon\sigma') &= -1 + \epsilon\, W_\sigma(S(a)).
\end{aligned}$$

Hence $W_{\sigma'}(Sa) = W_\sigma(a)$. We have established that U acts as a permutation in phase space and is therefore Clifford by Lemma 63. □

4.7 Prime power dimensions

Wigner functions for quantum systems with prime power dimensions have received particular attention in the literature (most prominently in Ref. [39]). Once again, this is due to the fact that a finite field of order d exists exactly when d is the power of a prime and that the field's well-behaved geometrical properties facilitate many constructions. The present section briefly addresses the relationship between three natural approaches to Wigner functions for such systems. We assume the reader is already familiar with the definition of Weyl operators over Galois fields; a thorough introduction can be found in Refs. [39, 46].

Let $d = p^k$ for some prime number p. There are three natural ways of associating a configuration space to $\mathcal{H}$. These are

1. an n-dimensional vector space over $\mathbb{Z}_p$,
2. a one-dimensional module over $\mathbb{Z}_{p^n}$ or
3. a one-dimensional vector space over the Galois field $\mathbb{F}_{p^n}$ of order p^n.

The first and the second of these points of view have manifestly been covered in this paper. So far we neglected case 3, because – as we will see – it can be completely reduced to the first one.

Let us quickly gather some well-known facts on finite fields. If p is prime and n a positive integer, $\mathbb{F}_{p^n}$ denotes the unique finite field of order $d = p^n$. The simplest case

occurs for $n = 1$, when $\mathbb{F}_p \simeq \mathbb{Z}_p$. For $n > 1$, fields $\mathbb{F}_{p^n}$ are realized by *extending* $\mathbb{F}_p$, which is then referred to as the *base field*. Extension fields contain the base field as a subset. The extension field possesses the structure of an n-dimensional vector space over the base field. A set of elements of $\mathbb{F}_{p^n}$ is a *basis* if it spans the entire field under addition and $\mathbb{F}_p$-multiplication. After having chosen a basis $\{b_1, \ldots, b_n\}$, we can specify any element $f = \sum_i f^i b_i$ by its expansion coefficients $\{f^i\}$. The operation

$$\mathrm{Tr} f = \sum_{k=0}^{n-1} f^{p^k}$$

takes on values in the base field and is $\mathbb{F}_p$-linear. Therefore,

$$\langle f, g \rangle \mapsto \mathrm{Tr}(fg)$$

defines an $\mathbb{F}_p$-bilinear form. For any basis $\{b_i\}$, there exists a *dual basis* $\{b^i\}$ fulfilling the relation $\mathrm{Tr}(b^i b_j) = \delta_{i,j}$ (we do not use Einstein's summation convention). From now on, we assume that a basis b_i and a dual one b^i have been fixed.

Repeating the construction put forward in Section 4.2, we introduce the Hilbert space $\mathcal{H} = L^2(\mathbb{F}_{p^n})$, in other words, $\mathcal{H}$ is the span of $\{|q\rangle | q \in \mathbb{F}_{p^n}\}$. The choice of a basis induces a tensor structure on $\mathcal{H}$ via

$$|q\rangle = |\sum_i q^i b_i\rangle \mapsto \bigotimes_i |q^i\rangle.$$

We obtain a character of $\mathbb{F}_{p^n}$ by setting $\chi_{p^n}(f) = \chi_p(\mathrm{Tr} f)$. Note that for $n = 1$, $\chi_{p^n} = \chi_p$. Expanding momentum coordinates $p = \sum_j p_j b^j$, the character factors:

$$\chi(pq) = \chi_p\big(\sum_{i,j} p_j q^i \mathrm{Tr}(b_i b^j)\big) = \prod_i \chi_p(p_i q^i).$$

Similarly, the shift and multiply operators factor with respect to this tensor structure:

$$\begin{aligned} x(\sum_i q^i b_i)|\sum_j x^j b_j\rangle &= \bigotimes_i x^{(i)}(q^i)|x^i\rangle \\ z(\sum_i p_i b^i)|\sum_j x^j b_j\rangle &= \prod_i \chi_p(p_i x^i)|\sum_j x^j b_j\rangle \\ &= \bigotimes_i z^{(i)}(p_i)|x^i\rangle, \end{aligned}$$

where $x^{(i)}$ and $z^{(i)}$ act on the ith p-dimensional subsystem. A straight-forward computation along the lines just presented shows that both the Weyl operators and the phase space point operators factor:

$$\begin{aligned} w(p,q) &= \bigotimes_i w^{(i)}(p_i,q^i) = w(p_1,\ldots,p_n,q^1,\ldots,q^n) \\ A(p,q) &= \bigotimes_i A^{(i)}(p_i,q^i) = A(p_1,\ldots,p_n,q^1,\ldots,q^n). \end{aligned}$$

The above result thus states that the Wigner function induced by the choice $Q = \mathbb{F}_{p^n}$ coincides – up to re-labeling of the phase space points – with the one for $Q = \mathbb{F}_p^n$. In particular, both definitions give rise to the same set of states with a non-negative phase space distribution.

For stabilizer states, however, the situation is not as easy, as will be discussed subsequently. The preceding discussion suggests defining a map $\iota : \mathbb{F}_{p^n}^2 \to \mathbb{F}_p^{2n}$ by

$$(p,q) \mapsto (p_1,\ldots,p_n,q^1,\ldots,q^n)$$

(see Refs. [46, 87]). Let M be a maximal isotropic subspace of $\mathbb{F}_{p^n}^2$. It is readily verified that $\iota(M) \subset \mathbb{F}_p^{2n}$ is again isotropic and a subspace. Further, we have shown that the sets of Weyl operators $w(M)$ and $w(\iota(M))$ coincide and hence so do the stabilizer states $|M\rangle$ and $|\iota(M)\rangle$.

The converse is not true. ι^{-1} does not necessarily map $\mathbb{F}_p^{2n}$ subspaces to those of $\mathbb{F}_{p^n}^2$. More precisely, if $M \subset \mathbb{F}_p^{2n}$ is a subspace, then $\iota^{-1}(M)$ can easily be proven to be closed under addition, but will in general fail to be closed under $\mathbb{F}_{p^n}$-scalar multipli-

cation. This proves the remark made in the introduction, namely that the set of 'single-particle' (i.e. $\mathbb{F}_{p^n}^2$) stabilizer states is a true subset of corresponding 'multi-particle' set. The following subsection gives a quantitative account of the relation of the sets.

4.7.1 Counting stabilizer codes

We are going to count the number of stabilizer states of a system composed of n d-level particles. In fact, the computation given below is slightly more general in that it gives the number of k-dimensional *stabilizer codes* [40].

Stabilizer codes are generalizations of stabilizer states. Recall Eq. (4.17), where we showed that summing Weyl operators $w(m)$ over the elements m of a maximal isotropic subspace M of V yields a one-dimensional projection operator. It can be shown that if the requirement of maximality is dropped, the sum still evaluates to a projector. The range of this operator is the *stabilizer code* defined by M. The dimension m of M and the dimension k of the stabilizer code are related by $k = d^{n-m}$.

Theorem 54. (Number of isotropic subspaces) *Let V be a $2n$-dimensional symplectic vector space over $\mathbb{F}_d$, where d is the power of a prime. The number of m-dimensional isotropic subspaces of V is given by*

$$\mathrm{Iso}(n, m, d) = \begin{bmatrix} n \\ m \end{bmatrix}_d \prod_{i=0}^{m-1} (d^{n-i} + 1),$$

where the square brackets denote the Gaussian coefficients

$$\begin{bmatrix} n \\ m \end{bmatrix}_d = \prod_{i=0}^{m-1} \frac{d^{n-i} - 1}{d^{m-i} - 1}.$$

Proof. The proof is inspired by a method employed in Ref. [22] to solve a related problem. We count the number of linearly independent m-tuples consisting of mutual orthogonal vectors. Indeed, as the first vector v_1 we are free to choose any non-zero element of V. There are $d^{2n} - 1$ such choices. The second vector must lie in the symplectic complement of the span of the first vector $\langle v_1 \rangle^\perp$. Hence, v_2 can be chosen from a $2n - 1$-dimensional vector space, the only restriction being that $v_2 \notin \langle v_1 \rangle$. It

follows that there exist $d^{2n-1} - d^1$ possibilities for v_2. Inducting on this scheme gives

$$\prod_{i=0}^{m-1} (d^{2n-i} - d^i) \tag{4.25}$$

such tuples.

However, since two different tuples might correspond to the same isotropic space, Eq. (4.25) over-counted the subspaces. To take that fact into account, we must divide by the number of bases within an m-dimensional space. Arguing in a similar fashion as before, we arrive at $\prod_{i=0}^{m-1}(d^m - d^i)$ for the sought-for number (see also Ref. [22]). Division gives

$$\mathrm{Iso}(n, m, d) = \prod_{i=0}^{m-1} \frac{d^{2n-i} - d^i}{d^m - d^i} = \prod_{i=0}^{m-1} \frac{d^{2(n-i)} - 1}{d^{m-i} - 1}.$$

Expanding $d^{2(n-i)} - 1 = (d^{n-i} - 1)\,(d^{n-i} + 1)$ and using the definition of the Gaussian coefficients concludes the proof. □

Corollary 55. *The number of d^{n-m}-dimensional stabilizer codes defined on n d-level systems is*

$$\mathrm{Stabs}(n, m, d) \;=\; d^m \begin{bmatrix} n \\ m \end{bmatrix}_d \prod_{i=0}^{m-1} (d^{n-i} + 1).$$

In particular, the number of stabilizer states is

$$\mathrm{Stabs}(n, n, d) = d^n \prod_{i=1}^{n} (d^i + 1).$$

Proof. We only need to justify the pre-factor d^m. The defining Eq. (4.17) generates a projector onto a stabilizer code given an isotropic space M and a character $\chi([v, \cdot])$ on M. If $\dim M = m$, then there are $|M| = d^m$ distinct such characters (see Appendix 4.8.3). □

We can now compare the number of stabilizer states for n particles of dimension d

to the corresponding number for a single d^n-dimensional system:

$$\begin{aligned}\frac{\mathrm{Stabs}(n,n,d)}{\mathrm{Stabs}(1,1,d^n)} &= \frac{\prod_{i=1}^{n}(d^i+1)}{d^n+1} = \prod_{i=1}^{n-1}(d^i+1) \\ &\geq d^{\sum_{i=1}^{n-1} i} = d^{\frac{1}{2}(n^2-n)}.\end{aligned}$$

This is the super-exponential scaling mentioned in the introduction.

4.8 Appendix

4.8.1 Discrete Stone-von Neumann Theorem

This section generalizes well-known results for prime-power dimensions (see e.g. Ref. [80] and citations therein) to all odd d. The proof is based on some simple observations employing group representation theory. We state a preparing lemma beforehand.

Lemma 56. *The Weyl representation is irreducible.*

Proof. We compute

$$\begin{aligned}\frac{1}{|H(\mathbb{Z}_d^n)|}\sum_{\substack{a\in V,\\ t\in\mathbb{Z}_d}} |\operatorname{tr} w(a,t)|^2 &= d^{-(2n+1)}\sum_t |\operatorname{tr} w(0,t)|^2 \\ &= d^{-(2n+1)}\sum_t d^{2n} = 1\end{aligned}$$

which establishes irreducibility by a well-known criterion from group representation theory (see any textbook on that topic, e.g. [103]). □

Proof. (of Theorem 37) By the composition law Eq. (4.4) it is clear that $w'(p,q,t) := w(S(p,q),t)$ is a representation of the Heisenberg group which affords the same character (i.e. $\operatorname{tr} w(a,t) = \operatorname{tr} w'(a,t)$). The preceding lemma yields that w and w' are equivalent and thus the existence of $\mu(S)$ follows. Further,

$$\begin{aligned}\mu(S)\mu(T)w(p,q)\mu(T)^\dagger\mu(S)^\dagger &= \mu(S)w(T(p,q))\mu(S)^\dagger \\ &= w(S\,T(p,q)) \\ &= \mu(ST)w(p,q)\mu(ST)^\dagger.\end{aligned}$$

Because the Weyl matrices span the set of all operators, the last line fixes $\mu(ST)$ modulo a phase and we have proven the second assertion.

We turn to the last claim. Let S and c be as defined in Eq. (4.10). Using the commutation relations Eq. (4.4) and the fact that conjugation by unitaries leaves the center $\chi(t)\mathbb{1}$ of the Weyl representation invariant, it is easy to see that S must be an isometry in the sense that $[Sa, Sb] = [a, b]$. To proceed, consider the following calculation. On the one hand

$$\begin{aligned} Uw(a)w(b)U^\dagger &= Uw(a+b, 2^{-1}[a,b])U^\dagger \\ &= w(S(a+b), 2^{-1}[a,b])c(a+b), \end{aligned} \tag{4.26}$$

while on the other hand,

$$\begin{aligned} Uw(a)w(b)U^\dagger &= Uw(a)U^\dagger Uw(b) \\ &= w(Sa)w(Sb)c(a)c(b) \\ &= w(Sa+Sb, 2^{-1}[Sa,Sb])c(a)c(b). \end{aligned} \tag{4.27}$$

Comparing the last lines of Eqs. (4.26) and (4.27) one finds that S must be compatible with addition in $\mathbb{Z}_d^{2n}$ meaning that $S(a+b) = Sa + Sb$. Because $\mathbb{Z}_d$ is *cyclic* the preceding property implies that S is also compatible with scalar multiplication:

$$S(\lambda a) = S(a + \cdots + a) = S(a) + \cdots + S(a) = \lambda S(a).$$

Hence S is linear and therefore symplectic. Lastly, again using lines (4.26) and (4.27), we have that $c(a+b) = c(a)c(b)$ and conclude that c is a character. By Lemma 58, there exists an $a_0 \in V$ such that $c(\,\cdot\,) = \chi([a_0, S\,\cdot\,])$. Thus:

$$\begin{aligned} w(a_0)\mu(S)\, w(a)\, \mu(S)^\dagger w(a_0)^\dagger &= w(a_0)w(Sa)w(-a_0) \\ &= \chi([a_0, Sa])w(Sa) \\ &= c(a)w(Sa). \end{aligned}$$

□

4.8.2 Axiomatic Characterization of the Wigner function

The discussion in Section 4.2.4 should suggest that Definition 39 yields 'the' natural analogue of the original continuous Wigner function. However, to bolster that claim with more objective arguments, we establish that – at least in prime dimensions – the form is virtually determined by the property of Clifford covariance (Theorem 41).

Theorem 57. (Uniqueness) *Let d be an odd prime. Let $Q, V, \mathcal{H}$ be as usual. Consider a mapping W' that fulfills the following axioms.*

1. (Phase space) *W' is a linear mapping sending operators to functions on the phase space V.*

2. (Clifford covariance) *W' is covariant under the action of the Clifford group, in the sense of Theorem 41.*

Then $W'_\rho(p,q) = \lambda_1 W_\rho(p,q) + \lambda_2$ for two constants $\lambda_{1,2}$. If further,

3. (Marginal probabilities) *W' gives the correct marginal probabilities, as stated in Theorem 40.3,*

then $W'(p,q) = W(p,q)$.

Proof. Consider an alternative definition $\rho \mapsto W'_\rho$ of a Wigner function. Linearity implies the existence of a set of operators $\{A'(v)\}$ such that $W'(v) = d^{-n} \operatorname{tr}(A'(v)\rho)$. W' is covariant under the action of the Weyl operators if and only if $A'(v) = w(v)A'(0)w(v)^\dagger$. So the only degree of freedom left in the definition of W' is the choice of $A'(0)$. Again, one must require $A'(S\,v) = \mu(S)\,A(v)\,\mu(S)$ if Theorem 41 is to hold. In particular, because the origin 0 is a fixed point of any linear operation, $A'(0)$ must commute with all $\mu(S)$.

As a consequence, the old, unprimed Wigner function $W_{A'(0)}$ of $A'(0)$ stays fixed under any symplectic operation S. Since any two non-zero points of V can be mapped onto each other by a suitable symplectic matrix S, $W_{A'(v)}$ must be constant on all such points. So there are only two parameters free to be chosen: $W_{A'(0)}(0)$ and $W_{A'(0)}(v), v \neq 0$. Clearly, the set of all operators that comply with these constraints is spanned by $\mathbb{1}$ and $A(0)$:

$$A'(0) = \lambda_1\,\mathbb{1} + \lambda_2\,A(0). \tag{4.28}$$

The above decomposition implies the first statement of the Theorem.

As for the second claim, choose an $a \in V$. The projection operator $|a\rangle\langle a|$ is invariant under the action of Weyl operators of the form $w(p, 0)$. Thus, due to Clifford covariance, the Wigner function $W'_{|a\rangle}$ must be p-shift invariant: $W'_{|a\rangle}(p + p', q) = W'_{|a\rangle}(p, q)$. We required Theorem 40.3 to hold, hence

$$\sum_{p \in Q} W'_{|a\rangle}(p, 0) = d^n \, W'(0, 0) = \delta_{a,0}.$$

By Eq. (4.28) and Theorem 40.5 it follows that $W'(0, 0) = d^{-n}(\lambda_1 + \lambda_2 \delta_{a,0})$, yielding $\lambda_1 = 0, \lambda_2 = 1$. □

4.8.3 Characters and Complements

Consider a space $R = \mathbb{Z}_d^n$ with a bilinear form $\langle \cdot\,, \cdot \rangle : R \times R \to \mathbb{Z}_d$. For any $s \in R$ the function $r \mapsto \chi(\langle s, r\rangle)$ defines a character of R. The form is said to be *non-degenerate* if $\langle s, \cdot\,\rangle \neq \langle s', \cdot\,\rangle$ for distinct s, s'. The two spaces we are concerned with are Q with the canonical scalar product and V with the symplectic scalar product. Both can easily be checked to be non-degenerate.

The following lemma states a basic fact about spaces with non-degenerate forms. We repeat it for completeness.

Lemma 58. *Let $R = \mathbb{Z}_d^n$ with non-degenerate bilinear form $\langle \cdot\,, \cdot \rangle$. Any character ζ of R is of the form $\zeta(r) = \chi([s, r])$ for some unique $s \in R$.*

Proof. Addition gives V the structure of a finite abelian group. Therefore, $V \simeq V^*$, as is well-known (see e.g. Ref. [92]). So there are $|V|$ different characters of V, but equally many of the form $\chi([v, \cdot\,])$. □

If d is prime and M a subspace of V, the well-known relation $\dim M + \dim M^\perp = \dim V$ holds [61]. It is, however, no longer true in the general case. A counter-example can be constructed along the same lines as in Section 4.2.3. Still, an analogue exists as demonstrated below.

Theorem 59. *Let $R = \mathbb{Z}_d^n$ with non-degenerate bilinear form $\langle \cdot\,, \cdot \rangle$. If M denotes a subspace of R, then the 'complementarity relation' $|M|\,|M^\perp| = |R|$ holds.*

Proof. We will show that

$$M^{\perp} \simeq \big(V/M\big)^{*}. \tag{4.29}$$

For $m \in M^{\perp}$, the relation $[v] \mapsto \chi([m, v])$ defines a character of V/M, as can easily be verified. Let us denote the map $m \mapsto \chi([m, \cdot\,])$ by ι_1.

Conversely, given an element ζ of $\big(V/M\big)^{*}$, $v \mapsto \zeta([v])$ is a character of V. By Lemma 58 there exists a unique $w \in V$ such that $\zeta([v]) = \chi([w, v])$. If $m \in M$, then $\zeta([m]) = \zeta([0]) = 1$ and hence $w \in M^{\perp}$. Using the notions just introduced, we can define $\iota_2 : \big(V/M\big)^{*} \to M^{\perp}$ by $\zeta \mapsto w$.

It is simple to check that $\iota_2 = \iota_1^{-1}$. In particular, ι_1 is invertible and Eq. (4.29) follows.

With the help of Lagrange's Theorem, we can compute

$$\big|M^{\perp}\big| = \big|\big(V/M\big)^{*}\big| = |V/M| = |V|/|M|,$$

which concludes the proof. □

Corollary 60. *Let V, Q be defined as usual. Let M be an isotropic subspace of V and S be any subspace of Q.*

1. (Maximally isotropic spaces) *M is equal to its symplectic complement $M^{\perp}$ if and only if $|M| = d^n$.*

2. (Characters of subspaces) *Any character ζ of S can be written as $\zeta(s) = \chi(qs)$ for a suitable $q \in Q$.*

Proof. Claim 1 follows immediately from Theorem 59 and the fact that isotropic spaces are contained in their symplectic complement: $M \subset M^{\perp}$.

We turn to the second statement. In Lemma 48 we have argued that the characters of S which are expressable as $\chi(qs)$ stand in one-to-one correspondence to cosets in $Q/S^{\perp}$. But $|Q/S^{\perp}| = |S|$ and hence all characters are of that form. □

4.8.4 A geometric note

The proof of the Main Theorem makes use of the fact that for any vector $v \in V$, there exists a symplectic operation S that sends v to a vector of the form $(p, 0)$. Indeed, if d is

prime, any two vectors are similar, in the sense that they can be mapped onto each other by a symplectic matrix. Technically, this is a trivial incarnation of Witt's Lemma (see Ref. [8] for a formulation that is applicable in our context).

Once again the non-prime case poses additional difficulties. Recall that the *order* of a $v \in V$ is the least positive $\lambda \in \mathbb{Z}_d$ such that $\lambda\, v = 0$. It is easy to see that the order of a vector is left invariant by the action of invertible linear mappings. If d is a composite number (i.e. not prime), then $V = \mathbb{Z}_d^{2n}$ contains elements of different orders which cannot be related by a linear operation. However, one might conjecture that any two vectors of equal order are similar. This is the content of the following lemma. Some concepts used in the proof can be found in Refs. [61, 128].

Lemma 61. (Similarity) *Let $V = \mathbb{Z}_d^{2n}$. Let $a_1, a_2 \in V$ be two vectors with the same order. Then there exists a symplectic matrix S such that $Sa_1 = a_2$.*

Proof. We can slightly weaken the assumptions made about V. All we require for this proof is that V is a finite $\mathbb{Z}_d$-module with non-degenerate symplectic form $[\,\cdot\,,\,\cdot\,]$. It need not be of the form $\mathbb{Z}_d^{2n}$.

Let $v \in V$ be a vector of order d. As $v \mapsto \chi([v,\,\cdot\,])$ implements an isomorphism, $V \to V^*$, $\mathrm{ord}\left(\chi([v,\,\cdot\,])\right) = \mathrm{ord}(v) = d$. There hence exists a $w \in V$ such that $[v, w] = \lambda$ has order d. Any such number possesses a multiplicative inverse λ^{-1} modulo $\mathbb{Z}_d$ and hence $w' = \lambda^{-1}$ fulfills $[v, w'] = 1$. Vectors satisfying such a relation are said to be *hyperbolic couples*. Denote their span $\langle\{v, w'\}\rangle$ as H.

Set $V' := H^{\perp}$. By Theorem 59 $|V| = |H|\,|V'|$. Further, it is easy to see that $H^{\perp} \cap H = \{0\}$ and hence $V = H \oplus\!\!\!\!\!\!\bigcirc\; V'$, where $\oplus\!\!\!\!\!\!\bigcirc$ denotes the *orthogonal direct sum*. We claim that the symplectic inner product is non-degenerate on V'. Indeed, suppose there is a non-zero $v' \in V'$ such that $[v', w'] = 0$ for all $w' \in V'$. Then, by definition of V', $[h, w'] = 0$ for all $h \in H$ and therefore v' would be orthogonal on all vectors of V. Hence such a v' cannot exist by the non-degeneracy of $[\,\cdot\,,\,\cdot\,]$.

Note that V' fulfills the assumptions made about V at the beginning of the proof and has strictly smaller cardinality. Thus, we can induct on $|V|$ to obtain a decomposition

$$V = H_1 \oplus\!\!\!\!\!\!\bigcirc \ldots \oplus\!\!\!\!\!\!\bigcirc H_n$$

of V in terms of two-dimensional subspaces spanned by hyperbolic couples $\{v_i, w_i'\}$. We arrange these vectors as the columns of a matrix $S = (v_1, \ldots, v_n, w_1', \ldots, w_n')$. The construction of the couples $\{v_i, w_i'\}$ ensures that S is symplectic, as can easily be verified.

Now let $a_1, a_2 \in V$ be two vectors with maximal order. By the preceding discussion, there exists symplectic matrices S_i having a_i as their respective first column. Clearly, then $S_2 S_1^{-1} a_1 = a_2$.

Lastly, suppose $\mathrm{ord}(a_i) = k \leq d$. It is easy to see that $a_i' = k a_i / d$ are elements of V with maximal order. Further, if S maps a_1' to a_2', then also a_1 to a_2. □

Corollary 62. (Transitive action) *Let $|M_1, v_1\rangle$, $|M_2, v_2\rangle$ be stabilizer states. If their respective associated isotropic subspaces M_1, M_2 are spanned by vectors of maximal order, then there exists a Clifford operation relating these state vectors.*

Proof. Let $\{m_1^{(i)}, \ldots, m_n^{(i)}\}$, $i = 1, 2$ be bases of M_1 and M_2 respectively. Assume that all vectors have maximal order. It is simple to adapt the previous proof for constructing a symplectic matrix S sending $m_i^{(1)}$ to $m_i^{(2)}$. □

4.8.5 Some properties of the phase space point operators

Lemma 63. (Properties of the phase space point operators) *The phase space point operators fulfill the following relations*

$$\begin{aligned} A(a) &= w(2a)A(0), \\ A(a)A(b) &= w(2a - 2b), \\ \mathrm{tr}(A(u)\,A(v)\,A(w)) &= \chi([v,u] + [u,w] + [w,v]). \end{aligned}$$

Further, if U permutes the phase space point operators under conjugation

$$U A(v) U^\dagger = A(v')$$

for all $v \in V$, then U is Clifford.

Proof. Clifford covariance (Theorem 41) implies $A(a) = w(a)A(0)w(a)\dagger$. Using The-

orem 40.5 it is easy to see that $A(0)w(a)A(0) = w(-a)$ and $A(0)^2 = \mathbb{1}$. Hence

$$A(a) = w(a)A(0)w(-a)A(0)\,A(0) = w(2a)A(0)$$

proving the first relation. The second one follows.

For the proof of the third equation, we abbreviate $A(0)$ as A. Then

$$\begin{aligned}
& \operatorname{tr}\left(A(u)A(v)A(w)\right) \\
= \;& \operatorname{tr}(w(2u)A\,w(2v)A\,w(2w)A) \\
= \;& \operatorname{tr}(w(2u)w(-2v)w(2w)A^3) \\
= \;& \chi([u,-v]+[u-v,w])\operatorname{tr}(w(2(u-v+w))A) \\
= \;& \chi([v,u]+[u,w]+[w,v])\operatorname{tr}(A(u-v+w)).
\end{aligned}$$

It has been noted in Theorem 40.40 that phase space point operators have unit trace, which concludes the proof.

Lastly, suppose the action of U permutes phase space point operators. For any $a \in V$, we have

$$\begin{aligned}
Uw(a)U^\dagger &= Uw(2\,2^{-1}(a-0))U^\dagger \\
&= UA(a)U\,U^\dagger A(0)U^\dagger \\
&= A(a')A(0') \\
&= w(2(a'-0'))
\end{aligned}$$

for suitable $a', 0' \in V$. Hence U maps Weyl operators to Weyl operators and is thus Clifford by definition. □

5

Quantum Margulis expanders

5.1 Introduction

Motivated by the prominent role expander graphs play in theoretical computer science [58], quantum expanders have recently received a great deal of attention [5, 10, 11, 48, 50, 51, 67]. In chapter, we present an observation which allows for the simple explicit construction of such quantum expanders. The method relies heavily on quantum phase space techniques: Once familiar with this techniques, the result is an almost trivial corollary of the analogous classical statement. We further discuss continuous analogues of quantum expanders, where again, phase space methods render this an obvious generalization. Hence, the present note can equally be regarded as the presentation of a simple quantum expander, as as a short exposition of the strengths of the phase space formalism as such.

5.2 Preliminaries

5.2.1 Expanders

Expander graphs turn up in various areas of combinatorics and computer science (for all claims made in this section, the reader is referred to the excellent survey article Ref. [58]). They often come into play when one is concerned with a property which "typically" holds, but defies systematic understanding. A simple example is given by classical error correction codes. One can show that a randomly chosen code is extremely likely to have favorable properties, but it seems very difficult to come up with a deterministic construction of codes which are "as good as random". Expander graphs can be explicitly constructed, but capture some aspects of generic graphs. It turns out that this property can be used to de-randomize, e.g., the construction of codes or certain probabilistic algorithms.

The formal definition is straightforward. Consider a graph G with N vertices V, each having D neighbors (we allow for multiple links and self-links). There is an obvious way to define a random walk on the graph: At each time step, a particle initially located on a vertex v will be moved to one of the D neighbors of v with equal probability. The resulting Markov process is described by an $N \times N$ doubly stochastic matrix A.

The largest eigenvalue of A is $\lambda_1 = 1$, corresponding to the "totally mixed" eigenvector $(1, \ldots, 1)/N$. Let λ be the absolute value of the second largest (by absolute value) eigenvalue. A small value of λ means that the Markov process is strongly mixing, i.e., converges rapidly to the totally mixed state. We call G an (N, D, λ) *expander* if it is described by these parameters. The goal is to find families of expander graphs with arbitrarily many vertices N, but constant (and small) degree D and λ.

While the notion of an expander *graph* seems hard to quantize (see, however, Ref. [51]), it makes sense to look for quantum analogues of strongly mixing Markov processes with low degree. Indeed, we call a completely positive map Λ a (N, D, λ)-*quantum expander* if Λ can be expressed in terms of D Kraus operators acting on $\mathcal{B}(\mathbb{C}^N)$ and the absolute value of its second largest singular value is bounded from above by λ (here, $\mathcal{B}(\mathcal{H})$ denotes the space of linear operators acting on a linear space $\mathcal{H}$). Once more: The intuition is to have a quantum channel which can be written using few Kraus operators, but which rapidly sends any input to the completely mixed state under repeated invocation.[1]

Quantum expanders have been introduced independently in Ref. [50] for the purpose of constructing states of spin-chains with certain extremal entanglement and correlation properties, and in Ref. [11], where the problem was approached from a computer science perspective. Very recently, randomized [51] and explicit [10, 11, 48, 50] constructions of expanders have appeared in the literature.

The basic idea is implicit in earlier work [5].

5.2.2 Margulis expander

Margulis provided the first explicit construction of a family of expander graphs [76]. Their expansion properties can be verified by elementary (if tedious) means [58].

The vertices of Margulis' graph are given by the points of a $N \times N$-lattice.[2] We label the axes of the lattice by the elements of $\mathbb{Z}_N = \{0, \ldots, N-1\}$. Now consider the

[1] It follows directly from the definition of an (N, D, λ)-quantum expander that

$$\|\Lambda_N(\rho) - \mathbb{1}/N\|_2 \leq \lambda \|\rho - \mathbb{1}/N\|_2, \tag{5.1}$$

that is, each invocation of the quantum expander contracts the 2-norm distance to the maximally mixed state in $\mathbb{C}^N$ by at least λ.

[2] Note a slight inconsistency in our notation: the number of vertices in this case is N^2, not N.

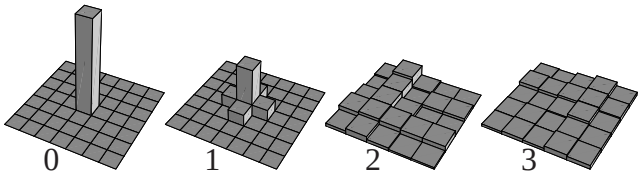


Figure 5.1: Phase space distributions resulting from three applications of the Margulis expander acting on a configuration initially concentrated at the origin of a 7×7 lattice. The starting distribution can be interpreted either as a classical particle with a well-defined position on a two-dimensional lattice, or as the quantum phase space operator $A(0,0)$ (see text for definition).

four affine transformations on $\mathbb{Z}_N^2$ given by

$$\begin{aligned} T_1 &: \quad v \mapsto S_1\, v, \\ T_2 &: \quad v \mapsto S_1\, v + (1,0)^T, \\ T_3 &: \quad v \mapsto S_2\, v, \\ T_4 &: \quad v \mapsto S_2\, v - (0,1)^T, \end{aligned} \tag{5.2}$$

where

$$S_1 = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, \quad S_2 = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}.$$

All operations are modulo N. Let $\mathcal{S}$ be the set of these four operations, together with their inverses. In Margulis' construction, two vertices are considered adjacent if and only if they can be mapped onto each other by an operation in $\mathcal{S}$.

One finds that λ is bounded above by $\sqrt{2}\,5/8$, independent of N [37, 58]. An instance of a random walk on the Margulis graph is visualized in Fig. 5.1.

5.2.3 Discrete phase space methods

Discrete quantum phase spaces have been discussed in detail in Chapter 4. In order to keep the present chapter as self-contained as possible, we give a very brief summary of the relevant methods.

The present section can be approached from a purely mathematical, or from a physically-oriented point of view. To make the argument more accessible, we will briefly outline both approaches before going into details.

Mathematically, one starts by noting that the operations T_i used in the construction of the Margulis graph (Eq. (5.2)) are affine transformations on $\mathbb{Z}_N^2$, where in addition the linear part S_i has unit-determinant. The functions of this kind form a finite group, which we will refer to as G_N. Two facts will be established below. Firstly,

- there is a (projective) unitary representation

$$T \mapsto U_T$$

  of G_N on $\mathbb{C}^N$.

This representation facilitates the quantization of the expander. Indeed, the quantum Margulis expander will be defined as the c.p. map Λ_N, which applies one of the unitaries $U_T, T \in \mathcal{S}$ at random. To prove that this construction defines an expander, we will need a second fact:

- Let N be odd. There are N^2 hermitian operators $A(a) \in \mathcal{B}(\mathbb{C}^N)$, labeled by the points $a \in \mathbb{Z}_N^2$, such that

  1. The operators form an orthonormal basis with respect to the Hilbert-Schmidt inner product:
  $$\frac{1}{N} \operatorname{tr}\big(A(v)\, A(w)\big) = \delta_{v,w}. \tag{5.3}$$

  2. The basis thus defined is compatible with the unitary representation of G_N in that
  $$U_T\, A(v)\, U_T^\dagger = A(T(v)), \tag{5.4}$$
  for $T \in G_N$, $v \in \mathbb{Z}_N^2$.

In order to analyze the action of Λ_N on a density operator ρ, we will use Eq. (5.3) to expand ρ in terms of the $A(a)$'s and then Eq. (5.4) to reduce the problem to the classical case (see Section 5.3).

Physically speaking, we will employ a phase space description of the quantum system. Recall that the term *phase space* originates in classical mechanics. Here, the state of a single particle in one spatial dimension is completely specified by two real parameters: its position and its momentum. The two-dimensional real vector space spanned

by the position and the momentum axes is referred to as the particle's phase space. Likewise, the state of a single quantum system can be specified by a quasi-probability distribution on phase space, namely the particle's Wigner function. The Wigner function shares many properties of classical probability distributions, except for the fact that it can take negative values (see Chapt. 4).

In the context of continuous-variable systems, affine volume-preserving transformations of the phase space are known as *canonical transformations*. Let ρ be a density matrix and denote by $W_\rho(v)$ the associated Wigner function. It is well-known [13] that for every canonical transformation T, there is a unitary operator U_T which implements the map T in the sense that

$$W_{U_T \rho U_T^\dagger}(v) = W_\rho(T(v)).$$

As detailed below, a similar relation holds for finite-dimensional quantum systems, associated with discrete phase spaces. Indeed, the Wigner function of a density operator ρ turns out to be nothing but the collection of expansion coefficients of ρ with respect to the basis given in Eq. (5.3); canonical transformations are elements of G_N; and the correspondence $T \mapsto U_T$ is just the representation mentioned in the first paragraph of this section.

So in this physical language, the basic realization is that the building blocks of the Margulis scheme (Eq. (5.2)) are canonical transformations of a discrete phase space.

To make all this more precise, let N be odd[3], $\mathcal{H} = \mathbb{C}^N$ and assume that some basis $\{|0\rangle, \ldots, |N-1\rangle\}$ in $\mathcal{H}$ has been chosen. Let $\omega = e^{\frac{2\pi}{N} i}$ be an Nth root of unity. We define the *shift* and *boost* operators as the generalizations of the X and Z Pauli matrices by

$$x(q)|k\rangle = |k+q\rangle, \qquad z(p)|k\rangle = \omega^{pk}|k\rangle \tag{5.5}$$

(arithmetic is modulo N). The *Weyl operators* are

$$w(p,q) = \omega^{-2^{-1}pq} z(p)x(q), \tag{5.6}$$

[3]We restrict attention to odd dimensions, as the theory of discrete Wigner functions is much more well-behaved in this case.

where $2^{-1} = (N+1)/2$ is the multiplicative inverse of 2 modulo N. For vectors $a = (p, q) \in \mathbb{Z}_N^2$, we write $w(a)$ for $w(p, q)$. Let

$$A(0,0) : |x\rangle \mapsto |-x\rangle \tag{5.7}$$

be the *parity operator* and denote by $A(p, q)$ its translated version,

$$A(p,q) = w(p,q)\, A(0,0)\, w(p,q)^\dagger. \tag{5.8}$$

We will refer to the $A(p, q)$'s as *phase space operators*. One can check by direct calculation that Eq. (5.3) holds. The *Wigner function* of an operator ρ is the collection of the expansion coefficients of ρ with respect to the basis formed by the phase space operators. Formally:

$$W_\rho(p,q) = \frac{1}{N} \operatorname{tr}\big(A(p,q)\,\rho\big). \tag{5.9}$$

There are two symmetries associated with a phase space: translations and volume-preserving linear operations. We shortly look at both in turn. Firstly, it is simple to verify that for $a, b \in \mathbb{Z}_N^2$

$$w(a)\, A(b)\, w(a)^\dagger = A(a+b). \tag{5.10}$$

Hence, Weyl operators implement translations on phase space. Secondly, let S be a unit-determinant matrix with entries in $\mathbb{Z}_N$. It turns out (c.f. Chapt. 4) that there exists a unitary operator $\mu(S)$ such that, for all $a \in \mathbb{Z}_N^2$ the relation

$$\mu(S)\, A(a)\, \mu(S)^\dagger = A(S\,a) \tag{5.11}$$

holds[4].

It follows immediately that for every affine transformation T of the type given in

[4]The operator $\mu(S)$ is the *metaplectic representation* of the symplectic matrix S. In quantum information theory, the set $\{w(a)\,\mu(S) \,:\, a \in \mathbb{Z}_N^2, \det(S) = 1\}$ is called the *Clifford group* [40], which must to be confused with the Clifford group appearing in the context of Fermions or representation theory of $SO(n)$.

Eq. (5.2), there exists a unitary operator U_T such that

$$W_{U_T \rho U_T^\dagger}(a) = W_\rho(T^{-1}(a)). \tag{5.12}$$

Hence, one can unitarily implement the building blocks of Margulis' random walk.

5.3 A quantum Margulis expander

With these preparations, it is obvious how to proceed. Define the completely positive map Λ_N by

$$\Lambda_N(\rho) = \frac{1}{|\mathcal{S}|} \sum_{T \in \mathcal{S}} U_T \, \rho \, U_T^\dagger, \tag{5.13}$$

where we have used the notation defined in Eq. (5.12) above. One immediately gets:

Observation 64 (Quantum Margulis expander)**.** *For odd N, the map Λ_N (Eq. (5.13)) acts on Wigner functions in the same way the Margulis expander acts on classical probability distributions. In particular, its degree and its spectrum are identical to the ones of the Margulis random walk. The Wigner functions of Λ's eigen-operators are the eigen-distributions of the classical random walk.*

Proof. Let $\Lambda_N^{(C)}$ be the stochastic matrix associated with the random walk on the classical Margulis graph. For $v \in \mathbb{Z}_N^2$, let $e(v)$ be the function on $\mathbb{Z}_N^2$, which takes the value 1 at v and 0 else. Clearly, the set $\{e(v)\}_{v \in \mathbb{Z}_N^2}$ spans the space of all functions on the lattice. Also,

$$\Lambda_N^{(C)}(e(v)) = \frac{1}{|\mathcal{S}|} \sum_{T \in \mathcal{S}} e(T(v)).$$

Using Eqs. (5.12, 5.13), we get for the quantum version

$$\Lambda_N(A(v)) = \frac{1}{|\mathcal{S}|} \sum_{T \in \mathcal{S}} A(T(v)).$$

Hence the action of the classical and the quantum expanders are identical on a basis. The claims follow. □

5.4 Efficient implementation

Consider a quantum expander which acts on a tensor-product Hilbert space $(\mathbb{C}^d)^{\otimes n} \simeq \mathbb{C}^N$ for $N = d^n$. The expander is *efficient* if it can be realized using $\mathrm{poly}(n)$ single-qudit or two-qudit quantum gates. So far, only two efficient constructions have been published [10, 48]. The Margulis expander adds to this list.

Theorem 65 (Efficient implementation)**.** *The quantized Margulis expander acts efficiently on* $(\mathbb{C}^d)^{\otimes n}$.

To establish the claim, we need to clarify how we introduce a tensor product structure in $\mathbb{C}^N$. Every $0 \leq j \leq N-1$ can be expressed in a d-adic expansion as $j = j_1 \ldots j_n$ for $0 \leq j_l \leq d$. More precisely, $j = \sum_{l=1}^{n} j_l d^{n-l}$. The tensor product structure is now given by $|j\rangle = |j_1\rangle \otimes \cdots \otimes |j_n\rangle$.

Lemma 66 (Efficient constituents)**.** *Let* $N = d^n$. *The following operators act efficiently on* $\mathbb{C}^N$*:*

1. *The quantum Fourier transform*

$$F : |j\rangle \mapsto N^{-1/2} \sum_{k=0}^{N-1} \exp\big(i\frac{2\pi}{N}\, jk\big)|k\rangle.$$

2. *The Weyl operators* $w(1,0)$ *and* $w(0,1)$.

3. *The operators* $\mu(T_1)$ *and* $\mu(T_2)$.

Proof. The first statement is well-known. See Chapter 5 in Ref. [82] for the qubit version, which can easily be adapted to general d. Next, consider $w(1,0) = z(1)$. We have

$$\begin{aligned} z(1)|j\rangle &= \exp\big(i\frac{2\pi}{d^n}\, j\big)|j_1, \ldots, j_n\rangle \\ &= \exp\big(i2\pi \sum_{l=1}^{n} j_l d^{-l}\big)|j_1, \ldots, j_n\rangle \\ &= \bigotimes_l \exp\big(i2\pi\, j_l d^{-l}\big)|j_l\rangle. \end{aligned}$$

Hence $z(1)$ is actually local. One confirms that $x(1) = F\, z(1)\, F^\dagger$ and thus $x(1)$ is efficient.

To conclude the proof, we need to borrow three statements from the theory of metaplectic representations. Firstly, μ is a projective representation[5], i.e.,

$$\mu(ST) = e^{i\phi(S,T)}\, \mu(S)\mu(T)$$

for some phase $\phi(S,T)$ (c.f. Chapt. 4). Secondly,

$$F = \mu\Big(\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \Big),$$

and thirdly,

$$U_\pm = \mu\Big(\begin{bmatrix} 1 & \pm 2 \\ 0 & 1 \end{bmatrix} \Big)$$

is given by

$$U_\pm |j\rangle = \exp(i2\pi/N\, (\mp j^2))\, |j\rangle.$$

The last two statements can be found in Theorem 4.1 of [80] (strictly speaking only for the case of prime N, but the proofs work for any odd value) or in Lemma 2 to Lemma 4 of [7]. The claim becomes easy to verify:

$$\begin{aligned} U_\pm |j\rangle &= \exp\big(i2\pi\, (\mp \sum_{l,l'=1}^{n} j_l j_{l'} d^{n-l-l'})\big)\, |j\rangle \\ &= \prod_{l,l'} R(l,l')|j\rangle, \end{aligned}$$

where we have introduced the diagonal two-qudit unitary

$$R(l,l')|j_l, j_{l'}\rangle = \exp(i2\pi\, (\mp j_l j_{l'} d^{n-l-l'}))\, |j_l, j_{l'}\rangle.$$

[5] Actually, μ is even a *faithful* representation, but that fact is irrelevant for our purposes.

Thus $U_\pm$ – and therefore in particular $\mu(T_1)$ – are efficient. Finally,

$$T_2 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}^3,$$

which implies that $\mu(T_2) \propto FU_-F^3$ is efficient. □

The proof of Theorem 65 is now immediate, as all the U_T's which appear in the construction of Λ can be implemented by combining the unitaries treated in the above lemma and their inverses.

5.5 Continuous variable systems

The quantum phase space terminology of Section 5.2.3 has originally been introduced in the context of continuous variable systems (see e.g. Ref. [85]. In particular, if we re-interpret the affine transformations $\mathcal{S}$ given in Eq. (5.2) as operations on $\mathbb{R}^2$, we immediately obtain a completely positive map Λ_∞ acting on the infinite-dimensional Hilbert space of a single mode. Does it constitute a quantum expander? After reviewing some definitions in Section 5.5.1, we will give an affirmative answer in Section 5.5.2. The action of expanders on second moments is discussed in Section 5.5.3.

5.5.1 Continuous phase space methods

In the continuous case, the phase space is given by $\mathbb{R}^2$. Let X and P be the canonical position and momentum operators. The Weyl operators [13, 34, 85] are now

$$w(p,q) = \exp(iqP - ipX). \tag{5.14}$$

As in Eq. (5.7), the parity operator $A(0,0)$ acts on state vectors $\psi \in L^2(\mathbb{R})$ as

$$(A(0,0)\psi)(x) = \psi(-x).$$

We define the phase space operators $A(p,q)$ for $(p,q) \in \mathbb{R}^2$ exactly as in Eq. (5.8). The Wigner function becomes

$$W_\rho(p,q) = \pi^{-1} \operatorname{tr}\left(A(p,q)\,\rho\right)$$

c.f. Eq. (5.9). The obvious equivalents of Eqs. (5.10,5.11) hold for $a \in \mathbb{R}^2$ and $S \in \mathrm{Sp}(2,\mathbb{R})$, the group of unit-determinant transformations of the two-dimensional real plane. Hence it is plain how to interpret Eq. (5.12) and finally how to turn Eq. (5.13) into a definition of Λ_∞, the infinite-dimensional quantum Margulis map.

5.5.2 A continuous quantum Margulis expander

A slight technical problem arises when transferring the definition of an expander to the infinite-dimensional case: both the invariant distribution $f(v) = 1$ of a classical expander and the invariant operator $\mathbb{1}$ of a quantum expander map are not normalizable. Hence, if we define e.g. the action of a completely positive map Λ on the set of trace-class operators $\mathcal{T}^1(\mathcal{H})$, the would-be eigenvector with eigenvalue 1 is not even in the domain of definition. In the light of this problem, we switch to the following definition of a quantum expander, which is compatible with the notion used up to now.

Definition 67. *Let $N \leq \infty$ and set $\mathcal{H} = \mathbb{C}^N$. A completely positive map Λ is an* (N, D, λ)-quantum expander *if, for all traceless operators $X \in \mathcal{T}^1(\mathcal{H})$,*

$$||\Lambda(X)||_2 \leq \lambda\, ||X||_2.$$

The definition above is best understood in terms of the Heisenberg picture:

$$|\operatorname{tr}(\Lambda^n(\rho)\, X)| = |\operatorname{tr}(\rho\, (\Lambda^\dagger)^n(X))| \leq \lambda^n$$

for all normalized ($||X||_2 = 1$), traceless observables X. Thus the state becomes "featureless" exponentially fast when being acted on by Λ. Let λ_M be the second largest eigenvalue of the finite Margulis expanders. Then:

Observation 68 (Continuous quantum expander)**.** *The infinite-dimensional quantum Margulis map Λ_∞ is an $(\infty, 8, \lambda_M)$-quantum expander.*

Note that by the previous section, we know there are $(N, 8, \lambda_M)$ quantum expanders for arbitrary high N. A priori, however, this does not imply the existence of a solution for $N = \infty$.

Once more, by switching to the phase-space picture, the proof of Observation 68 can be formulated completely in classical terms. The intuition behind the argument is simple to state. Take an element T of $\mathcal{S}$, e.g.

$$T : v \mapsto \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} v. \tag{5.15}$$

The inverse is given by

$$T^{-1} = \begin{bmatrix} 1 & -2 \\ 0 & 1 \end{bmatrix}, \tag{5.16}$$

regardless of whether the matrix is interpreted as acting on $\mathbb{R}^2$, $\mathbb{Z}^2$ or $\mathbb{Z}_N^2$. As the same is true for all other elements of $\mathcal{S}$, the action of the classical Margulis map "looks similar" on continuous, infinite discrete and on finite phase spaces – at least as long as it acts on distributions which are concentrated close to the origin, so that the cyclic boundary conditions of $\mathbb{Z}_N^2$ do not come into play. Using this insight, the following lemma reduces the continuous to the finite case.

Lemma 69. *Let $f \in C_0^0(\mathbb{R}^2)$ be a continuous function with compact support, such that*

$$\int_{\mathbb{R}^2} f(v)dv = 0. \tag{5.17}$$

Let $A : L^1(\mathbb{R}^2) \to L^1(\mathbb{R}^2)$ be the classical Margulis map acting on distributions on $\mathbb{R}^2$. Then

$$||A(f)||_2 \leq \lambda_M ||f||_2. \tag{5.18}$$

Proof. We discretize the problem by partitioning $\mathbb{R}^2$ into a net of squares with side length δ. More specifically, for $(x, y) \in \mathbb{Z}^2$, let

$$Q_\delta(x, y) = [(x - 1/2)\delta, (x + 1/2)\delta] \times [(y - 1/2)\delta, (y + 1/2)\delta]$$

be the square with edge length δ centered around $(x\,\delta, y\,\delta) \in \mathbb{R}^2$. The discretized

version of f is $f_\delta : \mathbb{Z}^2 \to \mathbb{C}$ defined by

$$f_\delta(x,y) = \frac{1}{\delta^2} \int_{Q_\delta(x,y)} f(v) dv.$$

Note that $\sum_{x,y} f_\delta(x,y) = 0$. On $\mathbb{Z}^2$, we use the δ-dependent norm

$$||f_\delta||_2 = \big(\delta^2 \sum_{x,y} |f_\delta(x,y)|^2 \big)^{1/2}$$

(the factor δ^2 corresponds, of course, to the volume of the squares $Q_\delta(x,y)$). Now, let T be one of the affine transformations in $\mathcal{S}$. We can interpret T as an operation on $\mathbb{Z}^2$ and define its action on f_δ accordingly by

$$(T(f_\delta))(x,y) = f_\delta(T^{-1}(x,y)).$$

For small enough δ, the approximation is going to be arbitrarily good: using the uniform continuity of f, and the fact that all $T \in \mathcal{S}$ are continuous and volume-preserving, one finds that for every $\varepsilon > 0$, there is a $\delta > 0$ such that simultaneously

$$\big|\, ||f_\delta||_2 - ||f||_2 \,\big| \;<\; \varepsilon/2, \tag{5.19}$$

$$\big|\, ||A(f_\delta)||_2 - ||A(f)||_2 \,\big| \;<\; \varepsilon/2. \tag{5.20}$$

As the support of f is compact, there is an $R \in \mathbb{N}$ such that $f_\delta(x,y)$ and $A(f_\delta)(x,y)$ are equal to zero whenever $|x| \geq R$ or $|y| \geq R$. This enables us to pass from $\mathbb{Z}^2$ to the finite lattice $\mathbb{Z}_N^2$ for $N > 2R$. Indeed, when we re-interpret f_δ as a function $\mathbb{Z}_N^2 \to \mathbb{C}$ and the $T \in \mathcal{S}$ as affine transformations on $\mathbb{Z}_N^2$, the values of $||f_\delta||_2$ and $||A(f_\delta)||_2$ remain unchanged. But we know that A is an $(N, 8, \lambda_M)$-expander for every finite N. Hence

$$||A(f_\delta)||_2 \leq \lambda_M ||f_\delta||_2,$$

implying (by Eqs. (5.19,5.20))

$$||A(f)||_2 \leq \lambda_M ||f||_2 - \varepsilon.$$

This proves the claim, as the right hand side can be chosen to be arbitrarily small. □

(of Observation 68). Once again, the quantum Margulis map Λ_∞ acts on the Wigner function W_X of any operator X in the same way the classical Margulis scheme acts on distributions on $\mathbb{R}^2$. Now, $X \in \mathcal{T}^1(\mathcal{H})$ implies $W_X \in L^2(\mathbb{R}^2)$. Because $C_0^0(\mathbb{R}^2)$ is dense in $L^2(\mathbb{R}^2)$ and Λ_∞ is continuous, Lemma 69 suffices to establish the claim. □

5.5.3 Action on second moments

In physics, one often measures the concentration of a phase space distribution by its second moments with respect to canonical coordinates. Thus, it may be interesting to look for signatures of the strong mixing properties of a quantum expander in its action on second moments.

More precisely, first moments are the expectation values of the position and momentum operators $(\langle X\rangle, \langle P\rangle)^T$ (where $\langle A\rangle = \mathrm{tr}(\rho A)$ for an operator A). The second moments are defined as the entries of the *covariance matrix*:

$$\gamma = 2\,\mathrm{Re}\begin{bmatrix} \langle X^2\rangle - \langle X\rangle^2 & \langle XP\rangle - \langle X\rangle\langle P\rangle \\ \langle PX\rangle - \langle X\rangle\langle P\rangle & \langle P^2\rangle - \langle P\rangle^2 \end{bmatrix}.$$

As the action of the continuous quantum expander in state space is defined via the metaplectic representation, the change in second moments can be computed explicitly. In particular, any $S \in \mathrm{Sp}(2,\mathbb{R})$ gives rise to a congruence $\gamma \mapsto S\gamma S^T$ for second moments. More generally, it is not difficult to see that for arbitrary convex combinations of states subject to affine transformations, the output's first and second moments depend only on the same moments of the input.

Under the Margulis random walk, one obtains for the first moments

$$\langle X\rangle \mapsto \frac{1}{|\mathcal{S}|}\sum_{T\in\mathcal{S}} x_T, \quad \langle P\rangle \mapsto \frac{1}{|\mathcal{S}|}\sum_{T\in\mathcal{S}} p_T$$

with $(x_T, p_T)^T = T(\langle X\rangle, \langle P\rangle)^T$. For the second moments:

$$\gamma \mapsto f(\gamma) := \sum_{i=1}^{2}\left(T_i\gamma T_i^T + T_i^{-1}\gamma(T_i^{-1})^T\right) + 2\,G, \tag{5.21}$$

where the matrix G is given by

$$G = \begin{bmatrix} \sum_T \frac{x_T^2}{|\mathcal{S}|} - (\sum_T \frac{x_T}{|\mathcal{S}|})^2 & \sum_T \frac{x_T p_T}{|\mathcal{S}|} - \sum_{T,T'} \frac{x_T p_{T'}}{|\mathcal{S}|^2}, \\ \sum_T \frac{x_T p_T}{|\mathcal{S}|} - \sum_{T,T'} \frac{x_T p_{T'}}{|\mathcal{S}|^2} & \sum_T \frac{p_T^2}{|\mathcal{S}|} - (\sum_T \frac{p_T}{|\mathcal{S}|})^2 \end{bmatrix}.$$

The latter matrix is evidently positive: Just write G as $G = AA^T$ with $A \in \mathbb{R}^{2,|\mathcal{S}|}$ with entries

$$A_{1,T} = \frac{x_T}{|\mathcal{S}|^{1/2}} - \sum_{T'} \frac{x'_T}{|\mathcal{S}|^{1/2}}, \tag{5.22}$$

$$A_{2,T} = \frac{p_T}{|\mathcal{S}|^{1/2}} - \sum_{T'} \frac{p'_T}{|\mathcal{S}|^{1/2}}. \tag{5.23}$$

To show that the main diagonal entries of $f^{(n)}(\gamma)$ diverge exponentially in the number n of applications of the map f, it is hence sufficient to consider the map

$$\gamma \mapsto g(\gamma) = \sum_{i=1}^{2} \Big(T_i \gamma T_i^T + T_i^{-1} \gamma (T_i^{-1})^T \Big),$$

since

$$f^{(n)}(\gamma) \geq g^{(n)}(\gamma).$$

A simple calculation yields

$$\gamma = \begin{bmatrix} a & b \\ b & c \end{bmatrix} \mapsto g(\gamma) = \begin{bmatrix} a+2c & b \\ b & c+2a \end{bmatrix}.$$

Let $\gamma^{(n)} = g^{(n)}(\gamma)$ be the covariance matrix after n iterations of g and define $\alpha = (a+c)/2$, and $\beta = (a-c)/2$ to simplify notation. Then

$$\gamma^{(n)} = \begin{bmatrix} 3^n \alpha + (-1)^n \beta & b \\ b & 3^n \alpha - (-1)^n \beta \end{bmatrix}.$$

This means that

$$\frac{1}{n}\log_3(\gamma^{(n)}) \;\rightarrow\; \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad (n \rightarrow \infty).$$

Thus, the elements of the main diagonal – and therefore also $\mathrm{tr}(f^{(n)}(\gamma)), \det(f^{(n)}(\gamma))$, and $\mathrm{spec}(f^{(n)}(\gamma))$ – diverge exponentially in the number n of iterations.

5.6 Summary and Outlook

Employing phase space methods, we were able to quantize a well-established combinatorial structure with almost no technical effort.

The unitaries which appear in the construction of expanders have randomization properties which are in some sense extremal. It would be interesting to see whether connections to other extremal sets of unitaries – e.g., *unitary designs* [28],[4] – can be found. Also, more practical applications may be anticipated, e.g., when one aims at initializing quantum systems in the maximally mixed state with few (i.e. D) operations, under repeated invocation of the same completely positive map Λ. Lastly, the programme may improve the understanding of iterated *randomization procedures*, as the one discussed in Ref. [106].

Acknowledgments

The author enjoyed stimulating discussions with, and the kind support of, more people than he can think of at the moment. A random selection includes A. Feito, A. Miyake, A. Serafini, C. Dawson, C. Mora, D.E. Browne, D. Gärtner, D. Plato, D. Schlingemann, E. Kashefi, F. Brandao, G. Toth, H.-J. Briegel, K. Audenaert, K. Kieling, J. Anders, J. Renes, M. Appleby, M.B. Plenio, M.M. Wolf, M. Müller, M. Van den Nest, N. de Beaudrap, S. Chaturvedi, S. Flammia, S. Virmani, T.J. Osborne, T. Felbinger, O. Dahlsten, and T. Rudolph. Thanks to you!

Jens, thanks for your friendship and support.

Publications

[1] J. Eisert and D. Gross. *Multi-particle entanglement.* In D. Bruss and G. Leuchs (Eds.) *Lectures on quantum information.* Wiley-VCH, Weinheim, 2006.

[2] D. Gross, *J. Math. Phys.*, **47**:122107, 2006.

[3] D. Gross, *Applied Physics B*, **86**:367, 2007.

[4] D. Gross, K. Audenaert, and J. Eisert, *J. Math. Phys.*, **48**:052104, 2007.

[5] D. Gross and M. Van den Nest, *Quant. Inf. Comp.*, **8**:263, 2008.

[6] D. Gross and J. Eisert, *Phys. Rev. Lett.*, **98**:220503, 2007.

[7] D. Gross and J. Eisert, *Quant. Inf. Comp.*, **8**:722, 2008.

[8] D. Gross, J. Eisert, N. Schuch, and D. Perez-Garcia, *Physical Review A*, **76**:052315, 2007.

[9] D. Gross, K. Kieling, and J. Eisert, *Physical Review A*, **74**:042343, 2006.

[10] K. Kieling, D. Gross, and J. Eisert, *New Journal of Physics*, **9**:200, 2007.

[11] K. Kieling, D. Gross, and J. Eisert, *Journal of the Optical Society of America B*, **24**:184, 2007.

[12] G. McConnell and D. Gross, *Quant. Inf. Comp.*, **8**:734, 2008.

[13] A. Serafini, O.C.O. Dahlsten, D. Gross, and M.B. Plenio, *Mathematical Systems Theory*, **40**:9551, 2007.

Bibliography

[1] S. Aaronson, *Proceedings of the Royal Society A*, **461**:3473, 2005, quant-ph/0412187.

[2] I. Affleck, T. Kennedy, E.H. Lieb, and H. Tasaki, *Commun. Math. Phys.*, **59**:799, 1987.

[3] D. Aharonov, W. van Dam, J. Kempe, Z. L, S. Lloyd, and O. Regev, quant-ph/0405098.

[4] P. Aliferis and D.W. Leung, *Phys. Rev. A*, **70**:062314, 2004.

[5] A. Ambainis and A. Smith, quant-ph/0404075.

[6] J. Anders and D.E. Browne, arXiv:0805.1002.

[7] D. Appleby, *J. Math. Phys.*, **46**:052107, 2005.

[8] M. Aschbacher. *Finite group theory*. Cambridge University Press, Cambridge, 1994.

[9] H. Barnum and N. Linden, *Journal of Physics A*, **34**:6787, 2001.

[10] A. Ben-Aroya, O. Schwartz, and A. Ta-Shma, arXiv.org:0709.0911.

[11] A. Ben-Aroya and A. Ta-Shma, quant-ph/0702129.

[12] I. Bengtsson and K. Zyczkowski. *Geometry of Quantum States: An Introduction to Quantum Entanglement*. Cambridge University Press, New York, NY, USA, 2006.

[13] S.L. Braunstein and P. van Loock, *Rev. Mod. Phys.*, **77**:513, 2005.

[14] S. Bravyi and R. Raussendorf, *Phys. Rev. A*, **76**:022304, 2007.

[15] G.K. Brennen and A. Miyake, arXiv:0803.1478.

[16] H.-J. Briegel and R. Raussendorf, *Phys. Rev. Lett.*, **86**:910, 2001.

[17] T. Bröcker and R. F. Werner, *J. Math. Phys.*, **36**:62, 1995.

[18] D.E. Browne and H.-J. Briegel, quant-ph/0603226.

[19] D.E. Browne, M.B. Plenio, and S.F. Huelga, *Phys. Rev. Lett.*, **91**:067901, 2003.

[20] D.E. Browne and T. Rudolph, *Phys. Rev. Lett.*, **95**:010501, 2005.

[21] C. Cabrillo, J.I. Cirac, P. Garcia-Fern, and P. Zoller, *Phys. Rev. A*, **59**:1025, 1999.

[22] P.J. Cameron. *Classical groups.* `http://www.maths.qmul.ac.uk/~pjc/class_gps/`.

[23] E. Campbell, J. Fitzsimons, S. Benjamin, and P. Kok, *New J. Phys.*, **9**:196, 2007.

[24] S. Chaturvedi, E. Ercolessi, G. Marmo, G. Mor, N. Mukunda, and R. Simon, *J. Phys. (Pramana)*, **65**:981, 2006.

[25] J.I. Cirac, W. Dür, B. Kraus, and M. Lewenstein, *Phys. Rev. Lett.*, **86**:544, 2001.

[26] D. Collins, N. Linden, and S. Popescu, *Phys. Rev. A*, **64**:032302, 2001.

[27] P. Cvitanovic, *Phys. Rev. D*, **14**:1536, 1976.

[28] C. Dankert, R. Cleve, J. Emerson, and E. Livine, quant-ph/0606161.

[29] V. Danos, E. Kashefi, and P. Panangaden, *J. ACM*, **54**:8, 2007.

[30] J. Dehaene and B. De Moor, *Physical Review A*, **68**:042318, 2003.

[31] W. Dür, L. Hartmann, M. Hein, M. Lewenstein, and H.J. Briegel, *Phys. Rev. Lett.*, **94**:097203, 2005.

[32] J. Eisert, *Phys. Rev. Lett.*, **95**:040502, 2005.

[33] J. Eisert, K. Jacobs, P. Papadopoulos, and M.B. Plenio, *Phys. Rev. A*, **62**:052317, 2000.

[34] J. Eisert and M.B. Plenio, *Int. J. Quant. Inf.*, **1**:479, 2003.

[35] M. Fannes, B. Nachtergaele, and R.F. Werner, *Commun. Math. Phys.*, **144**:443, 1992.

[36] G.B. Folland. *Harmonic Analysis in Phase Space*. Princeton University Press, Princeton, 1989.

[37] O. Gabber and Z. Galil, *J. Comput. System Sci.*, **22**:407, 1981.

[38] E. F. Galvao, *Phys. Rev. A*, **71**:042302, 2005.

[39] K. S. Gibbons, M. J. Hoffman, and W. K. Wootters, *Phys. Rev. A*, **70**:062101, 2004.

[40] D. Gottesman. *Stabilizer codes and quantum error correction*. PhD thesis, Caltech, 1997.

[41] D. Gottesman and I.L. Chuang, *Nature*, **402**:390, 1999.

[42] M. Grassl, A. Klappenecker, and M. Roetteler, quant-ph/0703112.

[43] R.B. Griffiths, S. Wu, L. Yu, and S.C. Cohen, *Phys. Rev. A*, **73**:052309, 2006.

[44] G. Grimmett. *Percolation*. Springer, Berlin, 1996.

[45] H. Groenewold, *Physica*, **12**:405, 1946.

[46] D. Gross. *Diploma Thesis, University of Potsdam (2005). Available online at* `http://gross.qipc.org`.

[47] H. Haffner, W. Hansel, CF Roos, J. Benhelm, D. Chek-al Kar, M. Chwalla, T. Korber, UD Rapol, M. Riebe, PO Schmidt, et al., *Nature*, **438**(7068):643, 2005.

[48] A.W. Harrow, *Quant. Inf. Comp.*, **8**:715, 2008.

[49] M.J. Hartmann, F.G.S.L. Br, and M.B. Plenio, *ao*, **2**:855, 2006.

[50] M.B. Hastings, *Phys. Rev. B*, **76**:035114, 2007.

[51] M.B. Hastings, *Phys. Rev. A*, **76**:032315, 2007.

[52] P. Hayden, D. Leung, P.W. Shor, and A. Winter, *Communications in Mathematical Physics*, **250**:371, 2004.

[53] P. Hayden, D.W. Leung, and A. Winter, *Communications in Mathematical Physics*, **265**:95, 2006.

[54] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest, and H.-J. Briegel, quant-ph/0602096.

[55] M. Hein, J. Eisert, and H.J. Briegel, *Phys. Rev. A*, **69**:062311, 2004.

[56] F. Hiai and D. Petz. *The Semicirlce Law, Free Random Variables and Entropy*. American Mathematical Society, 2000.

[57] A.S. Holevo, *Probab. Theory and Appl.*, page 133, 2005.

[58] S. Hoory, N. Linial, and A. Widgerson, *Bulletin of the American Mathematical Society*, **43**:439, 2006.

[59] E. Hostens, J. Dehaene, and B. De Moor., *Phys. Rev. A*, **71**:042315, 2005.

[60] R. L. Hudson, *Rep. Math. Phys.*, **6**:249, 1974.

[61] B. Huppert. *Endliche Gruppen*. Springer, Berlin, 1967.

[62] P. Jorr and S. Perdrix, quant-ph/0404125.

[63] R. Jozsa, quant-ph/0603163.

[64] R. Jozsa, *Quantum Information Processing: From Theory to Experiment*, 2006, quant-ph/0508124.

[65] R. Jozsa and N. Linden, *Proceedings: Mathematical, Physical and Engineering Sciences*, **459**:2011, 2003, quant-ph/0201143.

[66] A. Kenfack and K. Zyczkowski., *J. Opt. B*, **6**:396, 2004.

[67] I. Kerenidis and D. Nagaj, *J. Math. Phys.*, **47**:092102, 2006.

[68] K. Kieling, T. Rudolph, and J. Eisert, *Phys. Rev. Lett.*, 2007.

[69] C. King, K. Matsumoto, Mi. Nathanson, and M.B. Ruskai, quant-ph/0509126.

[70] A.Y. Kitaev, *Ann. Phys.*, **303**:2, 2003.

[71] A.B. Klimov and C. Muñoz, *J. Opt. B*, **7**:588, 2005.

[72] E. Knill, quant-ph/9608048.

[73] D. Kretschmann, D. Schlingemann, and R.F. Werner, quant-ph/0605009.

[74] U. Leonhardt, *Phys. Rev. A*, **53**:2998, 1996.

[75] O. M, M. Greiner, A. Widera, T. Rom, T.W. Hänsch, and I. Bloch, *Nature*, **425**:937, 2003.

[76] G. Margulis, *Problemy Peredaci Informacii*, **9**:71, 1973.

[77] V.D. Milman and G. Schechtman. *Asymptotic theory of finite dimensional normed spaces*. Springer-Verlag New York, Inc., New York, NY, USA, 1986.

[78] C. Miquel, J. P. Paz, and M. Saraceno, *Phys. Rev. A*, **65**:062309, 2002.

[79] C. Mora. *In preparation*, 2008.

[80] M. Neuhauser, *Journal of Lie Theory*, **12**:15, 2002.

[81] M.A. Nielsen, *Rep. Math. Phys.*, **57**:147, 2006.

[82] M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information*. Cambridge Unviersity Press, Cambridge, 2000.

[83] S. Östlund and S. Rommer, *Phys. Rev. Lett.*, **75**:3537, 1995.

[84] D. Perez-Garcia, F. Verstraete, M.M. Wolf, and J.I. Cirac, *Quant. Inf. Comp.*, **7**:401, 2007.

[85] D. Petz. *An invitation to the algebra of the canonical commutation relation*. Leuven University Press, Leuven, 1990.

[86] D. Petz and J. Reffy, arxiv:math/0310338.

[87] A. Pittenger and M. Rubin, *J. Phys. A*, **38**:6005, 2005.

[88] M. Popp, F. Verstraete, M.A. Martin-Delgado, and J.I. Cirac, *Phys. Rev. A*, **71**:042306, 2005.

[89] R. Raussendorf and H.-J. Briegel, *Phys. Rev. Lett.*, **86**:5188, 2001.

[90] R. Raussendorf and H.-J. Briegel, *Quant. Inf. Comp.*, **6**:433, 2002.

[91] R. Raussendorf, D.E. Browne, and H.J. Briegel, *Phys. Rev. A*, **68**:022312, 2003.

[92] W. Rudin. *Fourier analysis on groups*. Wiley-Interscience, New York, 1990.

[93] M.B. Ruskai, S. Szarek, and E. Werner, *Linear Algebra and its Applications*, **347**:159, 2002.

[94] M. Ruzzi, D. Galetti, and M.A. Machiolli, *J. Phys. A*, **38**:6239, 2005.

[95] W.P. Schleich. *Quantum Optics in Phase Space*. Wiley-VCH, 2001.

[96] D. Schlingemann, *Quant. Inf. Comp.*, **4**:287, 2004.

[97] D. Schlingemann and R.F. Werner, *Phys. Rev. A*, **65**:012308, 2002.

[98] U. Schollwöck, *Rev. Mod. Phys.*, **77**:259, 2005.

[99] B. Schumacher and R.F. Werner, quant-ph/0405174.

[100] Y.-Y. Shi, L.-M. Duan, and G. Vidal, *Phys. Rev. A*, **74**:022320, 2006.

[101] A. Shimony. Degree of Entanglement. In D.M. Greenberger and A. Zelinger, editors, *Fundamental Problems in Quantum Theory*, volume 755 of *New York Academy Sciences Annals*, page 675, 1995.

[102] P.W. Shor, *SIAM Rev.*, **41**(2):303–332, 1999.

[103] B. Simon. *Representation of finite and compact groups*. American Mathematical Society, Providence, Rhode Island, 1996.

[104] F. Soto and P. Claverie, *J. Math. Phys*, **24**:97, 1983.

[105] M.S. Tame, M. Paternostro, M.S. Kim, and V. Vedral, *Phys. Rev. A*, **73**:022309, 2006.

[106] G. Toth and J. Garcia-Ripoll, *Phys. Rev. A*, **75**:042311, 2007.

[107] M. van den Nest, W. Dür, A. Miyake, and H.J. Briegel, *New J. Phys.*, **9**:204, 2007.

[108] M. van den Nest, W. Dür, G. Vidal, and H.J. Briegel, *Phys. Rev. A*, **75**:012337, 2007.

[109] M. van den Nest, A. Miyake, W. Dür, and H.J. Briegel, *Phys. Rev. Lett.*, **97**:150504, 2006.

[110] B. Vaucher, A. Nunnenkamp, and D. Jaksch, *New Journal of Physics*, **10**(2):023005, February 2008, arXiv:0710.5099.

[111] F. Verstraete. *Private communication*.

[112] F. Verstraete and J.I. Cirac, cond-mat/0407066.

[113] F. Verstraete and J.I. Cirac, *Phys. Rev. A*, **70**:060302, 2004.

[114] F. Verstraete, M.M. Wolf, D. Perez-Garcia, and J.I. Cirac, *Phys. Rev. Lett.*, **96**:220601, 2006.

[115] G. Vidal, *Phys. Rev. Lett.*, **91**:147902, 2003.

[116] C.A. Munoz Villegas, A. Chavez Chavez, S. Chumakov, Y. Fofanov, and A.B. Klimov, quant-ph/0307051.

[117] A. Vourdas, *Rep. Prog. Phys.*, **67**:267, 2004.

[118] J. Walgate, A.J. Short, L. Hardy, and V. Vedral, *Phys. Rev. Lett.*, **85**:4972, 2000.

[119] D.F. Walls and G.J. Milburn. *Quantum Optics*. Springer-Verlag, Berlin, 1994.

[120] P. Walther, K.J. Resch, T. Rudolph, E. Schenck, H. Weinfurter, V. Vedral, M. Aspelmeyer, and A. Zeilinger, *Nature*, **434**:169, 2005.

[121] J. Watrous, arXiv.org:0804.3401.

[122] T.-C. Wei and P.M. Goldbart, *Phys. Rev. A*, **68**(4):042307, Oct 2003.

[123] A. Weil, *Acta Mathematica*, **111**:143, 1964.

[124] R. Werner, quant-ph/9504016.

[125] E. Wigner, *Phys. Rev.*, **40**:749, 1932.

[126] W. K. Wootters, *Ann. Phys. NY*, **176**:1, 1987.

[127] D.L. Zhou, B. Zeng, Z. Xu, and C.P. Sun, *Phys. Rev. A*, **68**:062303, 2003.

[128] É.M. Zmud, *Math. USSR Sbornik,* **15**:7, 1971.