PAPER • OPEN ACCESS

Jones index, secret sharing and total quantum dimension

IOP Publishing New J. Phys. 19 (2017) 023039 https://doi.org/10.1088/1367-2630/aa5c0c

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

OPEN ACCESS

RECEIVED
9 September 2016

REVISED
27 November 2016

ACCEPTED FOR PUBLICATION
25 January 2017

PUBLISHED
20 February 2017

PAPER

Jones index, secret sharing and total quantum dimension

Leander Fiedler[1,4], **Pieter Naaijkens**[2,3] **and Tobias J Osborne**[1]

[1] Institut für Theoretische Physik, Leibniz Universität Hannover, Germany
[2] Department of Mathematics, University of California, Davis, United States of America
[3] JARA Institute for Quantum Information, RWTH Aachen University, Germany
[4] Author to whom any correspondence should be addressed.

E-mail: leander.fiedler@itp.uni-hannover.de, pnaaijkens@math.ucdavis.edu and tobias.osborne@itp.uni-hannover.de

Keywords: quantum information, topological ordered states, thermodynamic limit, quantum dimension, secret sharing

Abstract

We study the total quantum dimension in the thermodynamic limit of topologically ordered systems. In particular, using the anyons (or superselection sectors) of such models, we define a secret sharing scheme, storing information invisible to a malicious party, and argue that the total quantum dimension quantifies how well we can perform this task. We then argue that this can be made mathematically rigorous using the index theory of subfactors, originally due to Jones and later extended by Kosaki and Longo. This theory provides us with a 'relative entropy' of two von Neumann algebras and a quantum channel, and we argue how these can be used to quantify how much classical information two parties can hide form an adversary. We also review the total quantum dimension in finite systems, in particular how it relates to topological entanglement entropy. It is known that the latter also has an interpretation in terms of secret sharing schemes, although this is shown by completely different methods from ours. Our work provides a different and independent take on this, which at the same time is completely mathematically rigorous. This complementary point of view might be beneficial, for example, when studying the stability of the total quantum dimension when the system is perturbed.

1. Introduction

Quantum phases can be understood as equivalence classes of ground states of quantum many body systems [1]. In this paper we are particularly interested in *gapped* quantum phases, up to quasiadiabatic evolution [2, 3]. A particularly interesting set of phases is that of topological ordered phases, i.e. classes of ground states that exhibit long-range entanglement. There are several different ways of setting up an equivalence of phases [1, 2, 4, 5], but in general they are expected to give rise to the same equivalence relation. It is believed that topological order is a property of states alone [5]. While defining the equivalence relation from physical principles is a task in itself, the characterisation of all possible equivalence classes is a much more subtle endeavour. One way of tackling this problem is to find invariants for the equivalence classes which can be computed locally and which allow one to distinguish different phases.

A possible candidate for an invariant is the topological entanglement entropy (TEE) [5, 6], which is believed to be a strong indicator of topological order. It is motivated by systems where the ground state satisfies an area law. In states with long-range entanglement, where this area law is expected to hold, the TEE is a correction of order $\mathcal{O}(1)$ to the von Neumann entropy of the reduced density matrix of the ground state on a disk shaped region. Furthermore, for the usual examples of anyonic systems, such as the toric code model [7] and the string-net models [8], it is proportional to $\log(\mathcal{D})$, where $\mathcal{D}$ is the total quantum dimension of the modular tensor category describing the anyons. The proportionality factor depends on the geometry of the bipartition of the system. The total quantum dimension itself characterises to some degree the anyonic nature of the local excitations of the ground state, as it is given by the quantum dimensions d_a of the different types of anyons via $\mathcal{D}^2 = \sum_a d_a^2$ [9]. A total quantum dimension that is larger than the number of distinct particles signifies non-abelian anyons [10], since an anyon a is abelian if and only if $d_a = 1$. The quantum dimension d_a of an anyon of

type a can be understood as the asymptotic growth of the Hilbert space that encodes n anyons a placed on a plane and conditioned on global vacuum (or trivial charge) [9].

In the thermodynamic limit of topologically ordered systems the total quantum dimension can be related to the Jones–Kosaki–Longo (JKL) index of certain inclusions of algebras of observables localised in cones [11]. Under precise (and natural) technical assumptions this index coincides with $\mathcal{D}^2$. The reason is that the JKL index gives us a way to compare the size of two (infinite dimensional!) algebras. As we shall see later, in our setting the big algebra is related to the smaller one precisely through 'charge transporters', which in turn are in correspondence with the different types of anyons. This suggests that there should be a connection between the JKL index and the TEE. However, it is *a priori* not clear how these very different concepts are related. Investigating this relation is one of the main goals of this paper.

In particular, we show with the example of the toric code how a secret sharing scheme for classical information between two parties naturally arises, and how we can relate it to the inclusion of algebras mentioned above. The amount of classical information that can be hidden with this scheme is then given by the JKL index. We compare this to a similar result in finite dimensions [12], where the TEE was shown to coincide with the optimal achievable rate of a (different) secret sharing scheme via the irreducible correlation. Based on this we argue that the JKL index is indeed closely related to the TEE. This picture is strengthened by the observation that the index is in a sense optimal and that it is related to a relative entropy between the corresponding von Neumann algebras. This is a generalisation of the relative entropy known from finite dimensional systems. Using this relative entropy and its relation to the index, we can interpret the index as a bound on the amount of classical information that can be encoded in the above secret sharing scheme.

1.1. Total quantum dimension and the TEE

An anyon model can be specified in terms of a set of *particle types*, together with a set of *fusion rules*, certain matrices describing the interchange of two anyons, i.e. the *braiding*, and tensors relating the different orders in which one can fuse n anyons. These rules have to satisfy certain compatibility conditions. Mathematically, this means an anyon model is described by a *modular tensor category* [13]. To each anyon type one can associate a quantum dimension d_i. One way to interpret this dimension is as a 'scaling factor' describing the asymptotic growth of the state space of n anyons of that type. It also describes the growth in ground-state degeneracy of a model when it is placed on an n-torus [14]. The *total quantum dimension* is defined as $\mathcal{D}^2 = \sum_i d_i^2$, where the sum is over all anyon types. In the language of tensor categories, $\mathcal{D}^2$ is called the (global) dimension of the category [15].

Based on arguments involving topological quantum field theory, Kitaev and Preskill [6] introduced a way to calculate the total quantum dimension: they defined an entropic quantity $S_{\text{top}}^{\text{KP}}$ and argued that it is equal to $\log \mathcal{D}$. Levin and Wen also defined a similar entropic quantity $S_{\text{top}}^{\text{LW}}$, and showed that $S_{\text{top}}^{\text{LW}} = \log \mathcal{D}^2$ for so-called quantum double models [5]. The difference of a factor of two between the two definitions can be attributed to the different shapes of the regions used in their definition.

The TEE has become a key tool in the study of topological order because it allows for a fairly practical approximation of the total quantum dimension: one only needs to solve the model on a torus large enough that the entropies for the various regions involved in its definition can be non-trivial [16]. Unfortunately the TEE does suffer from some shortcomings: it is far from clear how to extend it to higher dimensional systems (see, however [17] for recent progress) and situations involving symmetry protection [18] and it is also a deeply non-trivial task to show that it is stable under quasiadiabatic equivalence (for some partial progress see [19]). Another issue is that one can construct examples of states that appear to have a universal TEE term in their entanglement entropy but which are topologically trivial. One such example is due to Bravyi (see section 2.3 of [20] for a description).

1.2. Secret sharing

Secret sharing schemes can be seen as an instance of error correction codes. They are based on the idea that, given a set of states of the system, one needs access to a certain 'minimal' set of observables on the system in order to distinguish states in this set. This becomes particularly interesting when considering settings where information should be encoded in such a way that only observers, that can act on sufficiently large parts of the system are able to decode the hidden information. Classical secret sharing schemes where discussed in [21] and later generalised to the quantum setting in [22]. There are certain bounds on the amount of information that can be encoded in such schemes [22, 23], that is, bounds on the size of the regions (also called shares) and the minimal number required to decode the information, given the total system size. Here we consider secret sharing schemes in the context of topologically ordered states.

For topologically ordered systems, such as the toric code, the ground states of the Hamiltonian are locally indistinguishable [4]. That is, with access to observables that act on a few sites of the system only, it is not possible

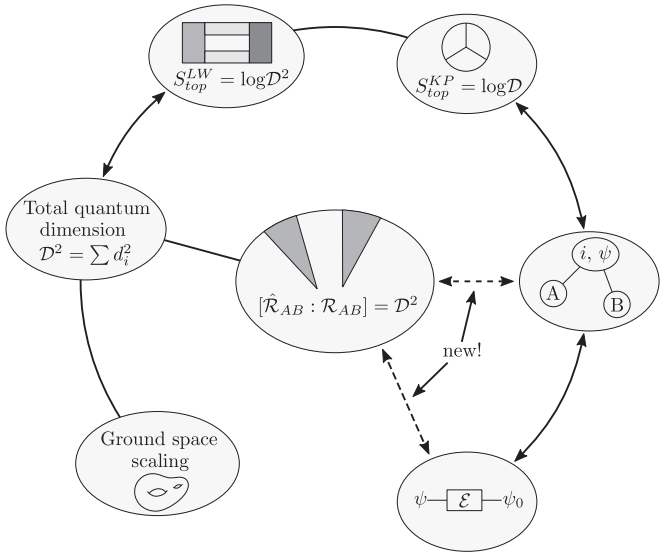

Figure 1. An anyon model has a total quantum dimension $\mathcal{D}^2$. The existence of anyons in models is related to long-range entanglement in the system. By judiciously choosing combinations of entanglement entropies of distinct regions, the entanglement due to topological order can be isolated. This leads to topological entanglement entropies $S_{\text{top}}^{\text{KL}}$ and $S_{\text{top}}^{\text{LW}}$, the differences being mainly due to the choice of regions. These entropies are argued to be related to the total quantum dimension $\mathcal{D}^2$ [5, 6]. The latter can be obtained as a Jones–Kosaki–Longo index associated to cone algebras [11]. In this paper we concentrate on the dashed arrows, arguing that by reinterpreting the topological entropy in terms of an information hiding task [12], it can be naturally connected to the cone index. The log of the index tells us something about how much information we can hide, and the index theory provides us with a channel $\mathcal{E}$ which describes the limited powers of an adversary Eve. Finally, $\mathcal{D}$ is related to the ground space degeneracy as a function of the genus of the surface on which the model is defined [14].

to distinguish the ground states. In order to do so one needs observables that act non-locally, that is, on a part of the system that is large compared to the system size. Note that this is exactly an error correction condition on the ground state space: local perturbations of the ground state can be detected and afterwards corrected. Hence, we can regard the ground state space as a quantum code, where the resulting size of the code space is determined by the total quantum dimension $\mathcal{D}$ of the anyon model and the genus of the manifold in which the system is embedded [7].

In the thermodynamic limit, however, locally indistinguishable states converge to the *same* state (in the weak*-topology), since their expectation values on local operators coincide as soon as the system size is big enough. Hence in that setting we cannot directly appeal to the degeneracy of the ground state space. Nevertheless, it should still be possible to use the topological charges to secretly share information between two parties in the system, if one restricts the corresponding regions in which the excitations are distributed accordingly. The intuition for this comes from the observation that in two dimensions excitations above the ground state always occur in conjugate pairs at the endpoints of a string, where the excitations do not depend on the exact geometry of the string but only on its endpoints. As long as one can 'keep' these endpoints 'away' from a possibly malicious third party by restricting their observables it should be impossible for them to determine which pair of excitation was created. The expected size of the code space is then again given by the total quantum dimension $\mathcal{D}$ of the anyon model. This forms the basis for our secret sharing scheme in the thermodynamic limit.

1.3. Content of this work

In this paper we try to connect the different approaches to obtain the total quantum dimension $\mathcal{D}$ and related quantities. In particular, we advocate an (operator) algebraic way to obtain the total quantum dimension $\mathcal{D}$, which will allow for generalisations to different dimensions and symmetry protected cases. In addition, we interpret $\mathcal{D}$ in terms of a information hiding task, making a direct connection between the TEE and the JKL index possible. Although we do not claim that our approach solves the problems with the TEE mentioned above, we believe it offers additional insight to the nature of topological order. In particular, as we formulate $\mathcal{D}$ in terms of observable algebras it is easier to anticipate a proof of the stability of the index under adiabatic equivalence and to extend it to more exotic scenarios. There are many ways to think about $\mathcal{D}$, some of which are outlined in figure 1. That figure also shows how our work fits into the big picture.

We will start in section 2 with explaining our intuition about the index at a finite dimensional variant, discuss drawbacks and problems that arise in the context of finite system sizes, and illustrate our intuition with the example of a chain of Fibonacci anyons. In section 3 we recall the necessary notions and properties of two

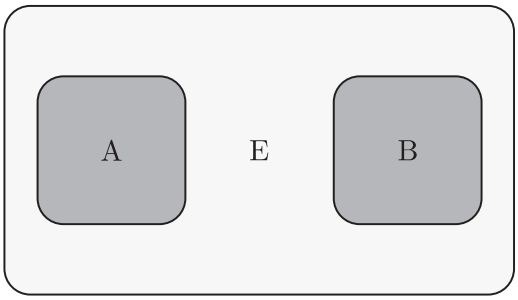

Figure 2. The system is partitioned into three parts: regions A and B controlled by Alice and Bob, and the rest (E), controlled by Eve.

dimensional models in the thermodynamic limit that we want to consider and discuss how the JKL index appears in this context. Section 4 then is devoted to constructing a secret sharing scheme in the example of the toric code on the infinite plane and to explaining how it relates to the index. Furthermore we discuss how this is connected to recent work [12], where for finite two-dimensional lattice systems it was shown that there is a connection between the TEE and the irreducible correlation of certain secret sharing schemes. We also discuss the role of superselection sectors in our construction.

One of the main contributions of our work is discussed in section 5. There we illustrate how index theory can be used to study the secret sharing scheme in the context of quantum information theory. In particular, one gets a quantum channel 'for free', and it is possible to define a relative entropy for certain algebras. Using this relative entropy the (logarithm of the) index can be recovered, and we see how this provides us with bounds on the amount of information that can be hidden in the secret sharing scheme. As we are mainly working in an algebraic setting, in section 6 we shed some light on how one can reformulate the picture of secret sharing schemes in terms of private subsystems of a channel between the corresponding algebras of observables, and give some of the details for the example of the toric code. Finally we remark on the stability of the index under local perturbations.

The goal of this work is to focus on the physical ideas and intuition behind our constructions. Many parts can be made mathematically rigorous, but this requires substantial mathematical machinery, in particular from the theory of von Neumann algebras. We refer to the relevant literature whenever this is the case. However, since we work in an operator-algebraic framework, some basic terminology of this field is unavoidable. The appendix contains a motivation on why we use this language to describe systems in the thermodynamic limit, as well as an introduction to the basic notions that we use in the course of this work.

2. Finite dimensions

To explain the main idea behind our index approach, we first consider a finite-dimensional variant. Although the main idea can be made clear in this case, it is a little surprising that a careful algebraic analysis seems infeasible, *precisely* because of the finite dimensionality. We return to this point later. Although the finite dimensional case is perhaps somewhat naive in light of these limitations, it nevertheless provides some intuition for the approach we take in the thermodynamic limit.

2.1. Motivation: a secret sharing task

The results in this section are not completely rigorous, but are intended as motivation for the (rigorous!) results in the thermodynamic limit, which we describe later. In the finite-dimensional 'toy model', the set-up is as follows. The system, defined on a lattice L, is divided into three parts A, B, and E, like in figure 2. Alice and Bob each control disjoint parts of the system, and Eve (perhaps some government agency) controls the rest. Suppose the system is initially in the state $|\Omega\rangle$. Alice and Bob have the task of storing a classical message in $|\Omega\rangle$; they want to use the system to set up something akin to a quantum I2P network which would be anonymous and immune from censorship. To achieve this task they are allowed to do *any* joint quantum operation on their respective regions A and B. In this case one can easily deduce that the configuration space for their anonymous and secret messages is given by

$$\mathcal{V}_{AB} := \mathrm{span}\{U_{AB}|\Omega\rangle \mid \mathrm{supp}(U_{AB}) \subset AB\}.$$

However, in achieving their information-hiding goal there is no reason we should restrict Alice's and Bob's operations to act only on AB. Indeed, they are allowed to touch sites belonging to Eve, *as long as Eve does not find out*. Clearly, in this finite-dimensional setting, this will be help if Eve is allowed to perform *any* bona fide

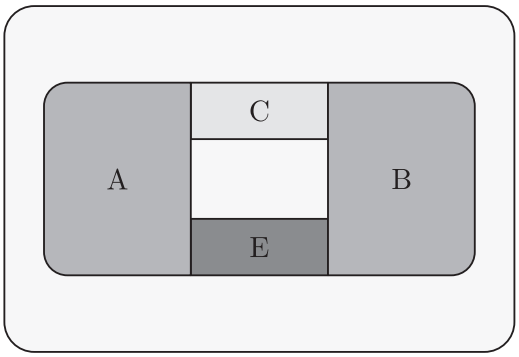

Figure 3. Alice and Bob control the regions A and B, but in addition have access to a region C, 'bridging' their parts. Eve on her part has access to a disjoint region E, small compared to the system size. Alice and Bob can change their choice of region C, according to Eve's choice of the region E.

quantum operation on her part of the system. However, if for some reason Eve's capabilities are restricted (e.g. perhaps government funding for building spying networks has been cut), there is a possibility for Alice and Bob to exploit this limitation and potentially hide more information in $|\Omega\rangle$. In this paper we postulate that Eve should only be able to do *local* measurements. Here 'local' means small compared to the system size, and compared to the regions that Alice and Bob control[5]. In particular, we disallow measurements that act on all sites on a ring around either Alice's or Bob's region (see figure 3). It will become clear from the example given below why we impose this restriction. Eve can do an unlimited number of such operations in succession, so long as the resulting operation does not encircle A or B[6].

Alice and Bob can do any joint operation on their part of the system and in that way can store a classical or quantum message that is inaccessible to Eve. Given that Eve has limited eavesdropping capabilities, the question is if this allows Alice and Bob to encode additional signals into $|\Omega\rangle$. This is the problem that we want to answer. To this end, consider the space $\widehat{\mathcal{V}}_{AB}$ generated by states that Eve cannot distinguish from $|\Omega\rangle$ by the operations at her disposal. If we denote $\mathcal{O}_E$ for the set of operations that Eve is allowed to perform, it can be defined as

$$\widehat{\mathcal{V}}_{AB} \coloneqq \mathrm{span}\{|\Omega_{ABE}\rangle \,|\, \langle\Omega_{ABE}|O_E|\Omega_{ABE}\rangle = \langle\Omega|O_E|\Omega\rangle,\ \forall\, O_E \in \mathcal{O}_E\}. \tag{1}$$

Note that this is precisely the statement that the space $\widehat{\mathcal{V}}_{AB}$ forms an error correction code that corrects the errors caused by Eve's observables $\mathcal{O}_E$ [24]. Clearly the Hilbert space $\mathcal{V}_{AB}$ is contained in $\widehat{\mathcal{V}}_{AB}$. Note that the condition on the expectation values above is nonlinear in the vectors of the form $U_{ABE}|\Omega\rangle$, so that it is not quite natural to take the linear span. For the models we have in mind, however, this is *does* make sense. A typical feature of these models is that the states corresponding to anyons of *distinct* type cannot be converted into each other with local operations (if the compensating anyonic excitations, which are necessarily there because of charge conservation, are localised far away). In other words, the anyons belong to different superselection sectors. Taking a superposition of such states, one sees that for local observables O_E the cross terms vanish when calculating the expectation value. This is essentially why this somewhat naive approach works in models such as the toric code.

We now have enough information to explain the calculation of the index invariant. This is given by the *ratio* of the dimensions of $\mathcal{V}_{AB}$ and $\widehat{\mathcal{V}}_{AB}$ of Alice's and Bob's regions:

$$[\widehat{\mathcal{V}}_{AB} : \mathcal{V}_{AB}] \coloneqq \frac{\dim \widehat{\mathcal{V}}_{AB}}{\dim \mathcal{V}_{AB}}. \tag{2}$$

We will later consider a different (and less naive) definition for this index in an operator-algebraic setting. For now we note that an equivalent way to express the index in this toy model is as a difference of entropies: here Alice and Bob are comparing the rates of two maximally mixed signal ensembles, one built from the Hilbert space $\mathcal{V}_{AB}$, namely $\rho_{AB} \coloneqq \mathbb{I}/\dim \mathcal{V}_{AB}$ and the one built from $\widehat{\mathcal{V}}_{AB}$, namely $\widehat{\rho}_{AB} \coloneqq \mathbb{I}/\dim \widehat{\mathcal{V}}_{AB}$:

$$\log [\widehat{\mathcal{V}}_{AB} : \mathcal{V}_{AB}] \coloneqq S(\widehat{\rho}_{AB}) - S(\rho_{AB}).$$

At this point we illustrate the task above by an example. Consider Kitaev's toric code [7]. In this model, one can create pairs of (anyonic) excitations by acting with path operators on a ground state. These paths are either drawn on the lattice or on the dual lattice, or a combination of the two. Using such a path operator F_ξ, Alice and Bob can create a pair of excitations, where one excitation is in Alice's part, while the other one belongs to Bob.

[5] Perhaps the best analogy here is that Alice and Bob control separate nation-size states that cannot be completely encircled by an antagonistic spying nation.

[6] Note that, in the finite case, the set $\mathcal{O}_E$ of Eve's observables *does not* obviously form an algebra.

The claim is that Eve, with the operations at her disposal, cannot detect that such a pair of excitations was created. Indeed, it is well known that the state $F_\xi|\Omega\rangle$, where $|\Omega\rangle$ is a ground state, only depends on the endpoints of ξ. Hence, since Eve can only do local measurements, one can always choose a path that avoids the support of Eve's measurement, in which case it is clear that Eve cannot detect it. Note that the only way to detect the excitations is to measure the total charge in a region by measuring the path operator corresponding to a Wilson loop enclosing the region. This is precisely how Alice and Bob can detect the presence of a charge in their respective parts of the system. Since in the toric code charge addition is done modulo two, and there are two fundamental charges (electric and magnetic), they have access to four times as many orthogonal states in $\widehat{\mathcal{V}}_{AB}$ relative to $\mathcal{V}_{AB}$ to hide information from Eve. Thus the index for this case is 4, which is the total quantum dimension for the toric code. Since Alice and Bob can only measure charges locally in their region, relative phases between the different charged states get lost upon measurement. Hence they can only retrieve four *classical* bits of information.

2.2. Problems with this approach

There are some drawbacks to this approach. They mainly stem from two causes: (i) the index quantity is not obviously independent of the regions A and B; and (ii) there is no clear algebraic structure underlying the set of allowed operations for Eve. Her local operations do *generate* an algebra, but this algebra is too big: it contains all operations on Eve's region. In some cases there *is* a natural choice of algebra: for example in the toric code one can choose the abelian algebra generated by all star and plaquette operators acting on E. However, in general it seems to be difficult to get a good handle on Eve's operations, and consequently, it is difficult to find out what all the allowed operations for Alice and Bob are. We argue below that these difficulties can be overcome by passing to the thermodynamic limit. This is the starting point of our analysis.

The naive analysis here can be refined by using techniques developed by Haah [25]. He considers ground states of local commuting projection Hamiltonians for which examples include Kitaev's toric code and the Levin–Wen models. His main goal is to define an invariant for such Hamiltonians that is stable with respect to local perturbations that do not close the gap. Part of his construction is to identify the different types of (anyonic) excitations in the model. As discussed above, such excitations are precisely what allow Alice and Bob to share classical information. A key ingredient in his construction are algebras associated to annuli. These algebras are obtained by looking at the observables supported on the annulus, and dividing out the observables that commute with all terms of the Hamiltonian supported on the annulus, i.e., those operators that do not create excitations in the annulus. This quotient algebra can then be decomposed into smaller algebras using projections which correspond to the different particle types. This construction is—in a sense—dual to ours outlined above. His procedure allows one to detect a single charge sitting inside the annulus. Since the total charge should be zero on the ground state space, the compensating charge can be thought of as sitting inside a different annulus. By growing (and deforming) the annuli on the outside, we can make them fill the entire space outside of the parts in the interior. Hence, we again have divided the system into three regions—Alice, Bob and Eve. The only difference is then that we are interested in which information can be hidden from Eve (i.e., which are invisible to her), while Haah considers all the charges that can be detected inside the annuli. These two notions are clearly related, but we will not pursue this connection any further in this paper.

2.3. The Fibonacci chain

Before we discuss the thermodynamic limit, we consider another example which sheds some light on the relation to the algebraic properties of the anyons (for example, given as a modular tensor category, see [13]). For concreteness, suppose that we have n anyons, fusing to the vacuum. A basis for such states can be conveniently represented in terms of fusion trees. The key point then is to define the appropriate notions of a local operation for Alice, Bob and Eve, given that they each control a fixed set of the anyons. To this end we follow the approach of [26]. Of the n anyons, Alice (Bob) controls a group of n_A (n_B) anyons, Eve the rest. These groups of anyons are assumed to have total charge given by labels ρ_A, ρ_B and ρ_E. The local operations are then precisely those operations on the respective groups of anyons that leave this total charge unchanged. We can then construct the spaces $\widehat{\mathcal{V}}_{AB}$ and $\mathcal{V}_{AB}$.

As an example we consider the Fibonacci model [27] with anyons 1, τ and assume that $\rho_A = \rho_B = \rho_E = 1$. The Hilbert space of the system is also called the *fusion space*. Its states describe the different ways that the anyons can fuse. In the Fibonacci chain there is only one non-trivial fusion rule: $\tau \otimes \tau = 1 \oplus \tau$. That is, if we fuse two τ anyons, we either get a τ anyon again, or the trivial anyon 1. A basis for the Hilbert space of the system can then be obtained by labelling all different ways n distinct τ anyons can fuse to the trivial anyon. This can be done conveniently with the help of fusion trees, which label the outcome of the fusion operations. In figure 4 we illustrated this with an example of a handful of anyons. In this example, the two left-most anyons fuse to a τ, while the fourth and fifth anyon fuse to the trivial charge. The order in which the fusion is performed should be the same for all basis elements, but is otherwise arbitrary. Choosing a different order amounts to a basis transformation [13].

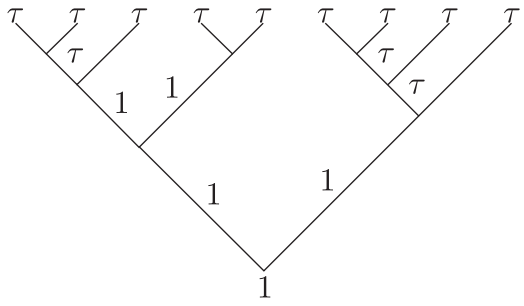

Figure 4. Consider a chain of n τ-anyons, grouped into three groups. Alice, Bob control the left and right group, Eve the ones in the middle. Since the fusion rules are $\tau \otimes \tau = 1 \oplus \tau$, these n anyons can fuse to the trivial charge 1. The states describing these different configurations span a vector space: the *fusion space*. A basis can be described by considering fusion trees as above. For example, the two leftmost τ anyons fuse to τ, while the two in the middle fuse to 1. Fusing the anyons in a different order would give a different basis, which is related to the old one by a unitary transformation.

Now choose a fusion tree where $\rho_A = \rho_B = \rho_E = 1$, that is, all Alice's anyons fuse to the trivial anyon, and the same is true for Bob and Eve. Write $|\Omega\rangle$ for the corresponding fusion state. If Alice and Bob act with local operations on the state $|\Omega\rangle$, they cannot change the total charge in their respective regions. That is, they can only make states such that Alice's anyons fuse to 1, and the same is true for Bob. By finding all fusion trees subject to these constraints we find the space $\mathcal{V}_{AB}$.

In contrast, if they are allowed to do non-local operations as well, there are additional possibilities: they can collude and make states such that the total charge in Alice's region and that in Bob's region is τ, but in such a way that these two τ's fuse to 1, so that the total charge of the system remains trivial. They can do this without changing the total charge of Eve (because two τ's can fuse to 1), so she is not able to detect this. This gives a bigger space $\widehat{\mathcal{V}}_{AB}$.

Finding the dimensions of $\mathcal{V}_{AB}$ and $\widehat{\mathcal{V}}_{AB}$ now reduces to the straightforward combinatorial task of counting all admissible fusion trees. If the number of anyons n_A and n_B tend to infinity, the ratio of the dimensions of these spaces tends to $1 + \varphi^2$, where φ is the golden ratio. This is precisely the total quantum dimension of the Fibonacci model. Of course, this is not a useful way to find the total quantum dimension, since this immediately follows from the given data. However, by considering this abstract setting it does shed more light on the secret sharing task, giving support to the definition in equation (2).

These different examples show that the essential step is to find the appropriate notion of what a local operation should be, emphasising that the algebraic point of view is a natural one.

3. Thermodynamic limit

To obtain a clear-cut, purely algebraic construction of the communication task described in the previous section we have to go to the thermodynamic limit. Instead of keeping track of the system size N, we start with infinitely many sites from the outset [28, 29]. The sites are labelled by a countable set $\mathbf{B}$. Typically, in the models we are interested in $\mathbf{B}$ is the set of edges (bonds) between nearest neighbours in a $\mathbb{Z}^2$ lattice or of a honeycomb lattice. For simplicity we assume that the local dimension is the same d for each site, but this can easily be generalised.

This setting is most conveniently described in the operator-algebraic framework, where the observables of the system are modelled by a C^*-algebra $\mathfrak{A}$. This can be thought of as the algebra of all observables (or, more general, operations) that can be approximated arbitrarily well (in norm) by observables that only act on a finite number of sites. We refer to appendix for an overview of the main definitions.

The results in this section are not new. Rather, we recall the main objects of interest in the operator-algebraic approach to topological phases, with a view towards our intended applications. Technical details can be found in [11, 30].

3.1. Alice, Bob and Eve again

We can divide the system into three parts again. Alice and Bob both control (disjoint) cone-like regions (see figure 5), and Eve controls the complement. We write Λ_E for the set of all sites that Eve controls, and similarly Λ_A and Λ_B for Alice's and Bob's cones. The corresponding observable algebras are denoted by $\mathfrak{A}(\Lambda_i)$. These are the algebras of all observables that can be approximated arbitrarily well in norm by observables acting on only finitely many sites inside Λ_i. The specific shape of the cones is not that important, as long as they are without holes, disjoint, and extend to infinity. It will become clear below why this choice of regions is natural.

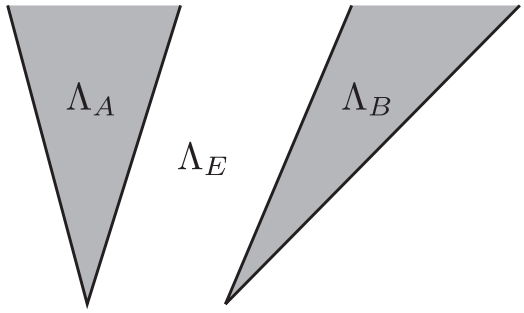

Figure 5. Alice and Bob each control infinite disjoint cone-like regions Λ_A and Λ_B, Eve controls the rest of the system.

We now suppose that $\mathfrak{A}$ is represented on some Hilbert space $\mathcal{H}$ by an irreducible representation π_0, that is $\pi_0(\mathfrak{A})$ is a C^*-subalgebra of $\mathfrak{B}(\mathcal{H})$. Which representation to use (in general, there are many inequivalent choices) is dictated by physical principles; in our case it will come from a pure, translation invariant ground state ω_0 via the GNS construction (see appendix for a short introduction). Motivated by the discussion above we postulate that Alice and Bob can perform every operation that commutes with all of Eve's local operations, hence this is given by $\widehat{\mathcal{R}}_{AB} \coloneqq \pi_0(\mathfrak{A}(\Lambda_E))'$. Recall that the prime denotes the commutant so that $\widehat{\mathcal{R}}_{AB}$ is the set of all bounded operators in $\mathfrak{B}(\mathcal{H})$ that commute with each $\pi_0(A)$, $A \in \mathfrak{A}(\Lambda_E)$. On the other hand we can consider all operations that Alice can implement on the cone she controls. These are given by the von Neumann algebra $\mathcal{R}_A \coloneqq \pi_0(\mathfrak{A}(\Lambda_A))''$. Taking the double commutant is natural here: it ensures that all the relevant spectral projections are in the algebra [28]. We define $\mathcal{R}_B$ similarly. The operations Alice and Bob can do together when only acting on their cones is then $\mathcal{R}_{AB} \coloneqq \mathcal{R}_A \vee \mathcal{R}_B$, where the wedge denotes the von Neumann algebra generated by the two algebras. Note that by locality, $\pi_0(\mathfrak{A}(\Lambda_A \cup \Lambda_B)) \subset \pi_0(\mathfrak{A}(\Lambda_E))'$. Taking commutants twice it follows that we have an inclusion $\mathcal{R}_{AB} \subset \widehat{\mathcal{R}}_{AB}$ of von Neumann algebras. The algebras are in fact factors, if one assumes that the ground state representation π_0 is irreducible (equivalently, ω_0 is a pure state), and $\mathcal{R}'_{AB} \cap \widehat{\mathcal{R}}_{AB} = \mathbb{C}I$ [11, Lemma 3.2]. Such an inclusion of von Neumann algebras is called an *irreducible subfactor*.

3.2. JKL index

We are interested in the question of which extra operations Alice and Bob can perform. These extra operations are precisely those that are in $\widehat{\mathcal{R}}_{AB}$ but not in $\mathcal{R}_{AB}$. Therefore we would like to know how much 'bigger' the algebra $\widehat{\mathcal{R}}_{AB}$ is compared to $\mathcal{R}_{AB}$. One way in which this can be quantified is by the Jones [31] (or rather, in our case, Kosaki–Longo [32]) index $[\widehat{\mathcal{R}}_{AB} : \mathcal{R}_{AB}]$ of inclusions of von Neumann algebras. It can be thought of as a generalisation of the index of a subgroup H in a group G. For our purposes, the technical details and properties behind this index (a subject on its own in operator algebra) play only a minor role. Rather, in the sequel we will focus on some properties that follow from the general theory, in particular the existence of a particular quantum channel and the Pimsner–Popa basis, a way to write elements of $\widehat{\mathcal{R}}_{AB}$ as a linear combination of a finite number of 'basis' elements with coefficients in the smaller algebra $\mathcal{R}_{AB}$.

If we assume two technical assumptions, the approximate split property (in [33] this property was referred to as the distal split property) and Haag duality [33, 34], it can be shown that the index does not decrease if one enlarges the cones. Haag duality (in a representation π_0) is a property of the commutants of cone algebras. In particular, it says that if Λ is a cone, $\pi_0(\mathfrak{A}(\Lambda))' = \pi_0(\mathfrak{A}(\Lambda^c))''$, where $\mathfrak{A}(\Lambda^c)$ is the algebra generated by all local observables outside of the cone. One inclusion follows easily from locality, but the other inclusion is non-trivial, and may fail in general. We will not give a precise definition here of the approximate split property (see [33] for the details), but in the present setting it amounts to saying that the map $AB \mapsto A \otimes B$, with $A \in \mathcal{R}_A$ and $B \in \mathcal{R}_B$ extends to an isomorphism $\mathcal{R}_{AB} \to \mathcal{R}_A \bar{\otimes} \mathcal{R}_B$ of von Neumann algebras, if A and B are two separated cones. When one thinks of finite dimensional systems this looks like a trivial statement, but in the thermodynamic limit it is not, and this property is related to deep operator-algebraic questions. For example, Longo used the split property in his solution to the factorial Stone-Weierstrass conjecture, which at the time was open for a long time [35]. One consequence is that if $\mathfrak{A} \subset \mathfrak{B}$ is an inclusion of C^*-algebras, then any factor state (in the sense that its GNS representation is a factor) of $\mathfrak{A}$ extends to a factor state of $\mathfrak{B}$. It also has been important in understanding entanglement properties in algebraic quantum field theory [36].

In general, we expect the index to be independent of the choice of cones (as long as their opening angles are big enough). In the next subsection it will become clear that the inclusion $\mathcal{R}_{AB} \subset \widehat{\mathcal{R}}_{AB}$ is related to the different charges of the model, and to operators that move them around. Keeping this in mind, independence of the index

on the choice of cones can be interpreted physically by saying that excitations can be localised well enough. That is, as long as the opening angle of the cone is not too small, each anyon can be localised in such a cone (regardless of the orientation of the cone). This can be shown explicitly for the toric code [11].

Note that the index is a property of the *state*, just like TEE. This is perhaps not apparent at first sight, but one should keep in mind that the respective algebras are taken in a specific representation π_0. This representation, in turn, usually is obtained from a state (in our case, generally a translation invariant ground state), and different states in general lead to different algebras (and possibly different values for the index).

3.3. Superselection sectors

In the finite-dimensional toy model we observed that the extra power that Alice and Bob have at their disposal is due to the existence of anyonic excitations which live in different superselection sectors. This is also true in the thermodynamic limit, where there is an elegant characterisation of such sectors. There they appear because there are inequivalent irreducible representations of $\mathfrak{A}$. This is equivalent to saying that vector states corresponding to distinct representations are not superposable, i.e. a relative phase between such vectors cannot be observed with any observable in $\mathfrak{A}$ [37].

Not all representations of $\mathfrak{A}$ are physically relevant. In the models we are interested in, charges are created by applying string-like operators. By moving one end of the string to infinity, we can obtain a state with a *single* charge. In topologically ordered models states created by such string-like operators only depend on the endpoints of the string. Hence the direction in which the charge is moved to infinity is not observable. In fact, if we restrict to operations outside an *arbitrary* cone containing the endpoint of the string, the charge cannot be detected at all and the system appears to be in the translationally invariant ground state. In other words, the charges can be localised in cones. Another natural condition is that we should be able to move the charges around.

On the level of representations π, these features are encoded by demanding that they satisfy the following criterion for all cones Λ:

$$\pi_0 \restriction \mathfrak{A}(\Lambda^c) \cong \pi \restriction \mathfrak{A}(\Lambda^c). \tag{3}$$

Here with $\restriction$ we mean that we restrict the representation to the subalgebra $\mathfrak{A}(\Lambda^c)$. That is, the criterion demands that if we restrict the representations π and π_0 to observables *outside* of a cone Λ, they become unitarily equivalent. Note that this restriction is important: for example, the representations π_0 and π are *not* equivalent if π describes a single anyonic excitation. That is, in such case there is no unitary V such that $\pi_0(A) = V\pi(A)V^*$ for all $A \in \mathfrak{A}$, but if we only require this to hold for $A \in \mathfrak{A}(\Lambda^c)$, such a unitary *does* exist. In algebraic quantum field theory a similar criterion is used, and it is known that (under some additional technical assumptions), studying these equivalence classes of representations allows one to find all relevant properties of the charges in the theory, for example their statistics and fusion rules [37]. Using similar ideas this can also be done for quantum lattice models, such as Kitaev's quantum double [30, 34].

How does this relate to the choice of the algebras $\mathcal{R}_{AB}$ and $\widehat{\mathcal{R}}_{AB}$? As in the finite dimensional setting, the idea is that Alice and Bob each control their own regions. The algebra $\mathcal{R}_{AB}$ describes the local operations they can perform. For example, it allows them measure the total charge in their region or move charges around. But it *does not* give them the ability to move a charge from one cone to the other, or equivalently, create a pair of conjugate charges (one in each cone). One can however show that *charge transporters* V that can move a charge from one cone into the other *are* contained in $\widehat{\mathcal{R}}_{AB}$. This shows that $\widehat{\mathcal{R}}_{AB}$ is bigger than $\mathcal{R}_{AB}$, and it is precisely the observation that it contains the charge transporters that will allow us to connect it to the quantum dimension.

4. Secret sharing

We now have the technical tools to describe a version of the quantum information task of section 2 in the thermodynamic limit. In particular, we will describe how we can use charges localised in cones to store data that is invisible to Eve, using the presence of superselection sectors, and argue how our procedure is related to the TEE.

In section 2 we described how an information hiding-task can be implemented for systems on a finite lattice in two dimensions, motivating our index approach. Although the naive method there works, this finite dimensional description suffers from drawbacks, such as the index described there not manifestly being independent of the regions A and B and that the set of allowed operations for Eve not carrying a nice algebraic structure. Here we describe an analogous setting in the thermodynamic limit of the toric code on the plane and show that it overcomes both drawbacks, while still resulting in an operationally sensible picture.

As in the finite dimensional variant, the task for Alice and Bob is to share information encoded in some quantum state on the whole system in such a way that Eve cannot access this information with any local measurement on her system. This means that Alice and Bob should be capable of reconstructing the shared

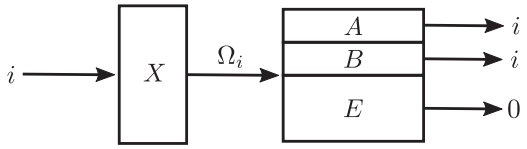

Figure 6. Example of a protocol for a secret sharing scheme: a sender X chooses a state Ω_i from the set of code states $\{\Omega_0 = \Omega, \Omega_X, \Omega_Z, \Omega_Y\}$ and sends it to the system consisting of authorised shares Alice (A) and (B) and unauthorised share Eve (E). The shares then operate locally on their part of the system to detect which state they received. The authorised shares Alice and Bob will be able to recover the information i of which state they received, whereas Eve will always get the same answer (0) no matter which state was sent.

information encoded in the quantum state just by performing local operations on their respective part of the system, while Eve cannot cannot access this information by using operations on her part of the system[7]. This is exactly the situation described by secret sharing schemes as treated in [23]. In such schemes the parts of the system that are capable of reconstructing the shared information solely by performing local operations are usually referred to as *authorised*, whereas those that cannot are called *unauthorised*. In our setting Alice and Bob will comprise the authorised parts of the system and Eve is unauthorised. Secret sharing schemes are usually defined for systems described by a finite dimensional Hilbert space, where the partition of the system into subsystems is given by a tensor product structure. In the thermodynamic limit of the toric code the system's Hilbert space is clearly infinite dimensional and the we do not have an obvious partition into tensor factors. In fact, one can show that the ground state Hilbert space does not factor [33] as $\mathcal{H}_\Lambda \otimes \mathcal{H}_{\Lambda^c}$, where $\mathcal{H}_\Lambda$ is the Hilbert space related to a cone[8]. In [23] it was shown, however, that there exists a characterisation of secret sharing schemes by error correction conditions. We will not generalise this secret sharing scheme to infinite dimensions, but will use this characterisation to illustrate that we indeed find a secret sharing scheme in the thermodynamic limit of the toric code. This is motivated by the observation that error correction schemes can be formulated in terms of operators [38] and, more generally, for von Neumann algebras [39].

We will briefly review the authorised and unauthorised sets comprising a secret sharing scheme in finite dimensions. Given a subspace $\mathcal{C} \subset \mathcal{K}$ of some n-partite Hilbert space $\mathcal{K}$, the authorised sets $A \subset \{1, \ldots, n\}$ are characterised by the condition that $\mathcal{C}$ corrects errors on their complements A^c. That is, for all $\phi, \psi \in \mathcal{C}$ and for all $E \in \mathfrak{B}(\mathcal{K}_{A^c})$ it holds that $\langle \phi, E\phi \rangle = \langle \psi, E\psi \rangle$. Unauthorised sets $U \subset \{1, \ldots, n\}$ are characterised by the condition that $\mathcal{C}$ corrects errors on them, i.e. $\langle \phi, F\phi \rangle = \langle \psi, F\psi \rangle$ for all $\phi, \psi \in \mathcal{C}$ and $F \in \mathfrak{B}(\mathcal{K}_U)$. For such pure state quantum secret sharing schemes it is easy to see that the no-cloning theorem implies that the unauthorised sets must be the complements of authorised sets and vice versa [23].

The setting we are considering here corresponds to the case where the shared information is classical. That is, the set of code states $\mathcal{C}$ consists of a choice of orthonormal vectors $\{\psi_i\}$. Then the conditions for unauthorised sets remain the same but the authorised sets A are characterised by demanding that for each pair of indices i, j and each operator $E \in \mathfrak{B}(\mathcal{K}_{A^c})$ it holds $\langle \psi_i, E\psi_j \rangle = \delta_{i,j} \langle \psi_j, E\psi_j \rangle$ [23]. Here it is no longer true that unauthorised sets have to be complements of authorised sets, for classical information can be cloned. Figure 6 shows what a protocol implementing a secret sharing scheme for classical information looks like. In the following section we describe how we can set up a secret sharing scheme in the thermodynamic limit of the toric code, specify a set of states which serve as code states, and check the above conditions.

4.1. The use of cones

We now come back to the thermodynamic limit and start by considering two disjoint cones Λ_A and Λ_B which are separated sufficiently far enough from each other[9]. For concreteness we describe the example of the toric code, but we believe that the method can be generalised to similar models; in particular Kitaev's quantum double models for abelian groups G can be handled directly by using results from [34]. These cones represent the regions to which Alice and Bob have access. The complement Λ_E of the union of these two cones is considered to be controlled by a (possibly malicious) third party Eve. Eve cannot access Λ_A or Λ_B. With the notations introduced in section 3 we denote the von Neumann algebras of observables localised in the cones Λ_A and Λ_B by $\mathcal{R}_A$ and $\mathcal{R}_B$. The von Neumann algebra generated by the local observables on Eve's part is written as $\mathcal{R}_E$, while the algebra of observables commuting with $\mathcal{R}_E$ is denoted $\widehat{\mathcal{R}}_{AB}$. Here we are working in the translation invariant

[7] If we speak of 'local' we always mean that the observable acts on finitely many particles on the lattice. Furthermore, in this context 'local' additionally means that the observable is localised in one of the cones.

[8] Although we do not claim that this is the case here, this touches upon a more fundamental property of infinite dimensional systems. Recently Slofstra has found a counterexample to Tsirelson's problem [60], by showing that there are commuting operator models for two-party correlations that are not equivalent to a tensor product model.

[9] In [33] this is defined rigorously for the toric code, and in [11] this is extended to more general models.

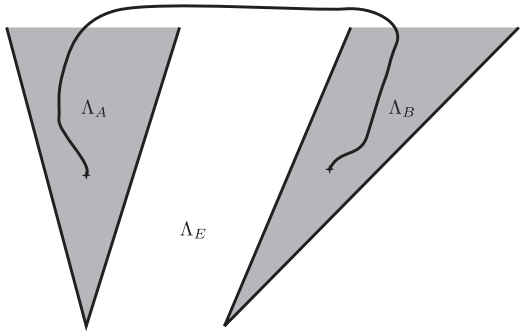

Figure 7. The cones Λ_A and Λ_B are the regions Alice and Bob have access to, and the remainder of the system Λ_E is controlled by Eve. The charge transporters between Λ_A and Λ_B are constructed from sequences of ribbons with fixed endpoints (one in each cone) such that with growing length the ribbons avoids finite sets in Λ_E. The solid line indicates an infinite ribbon that stretches out to infinity and which we can think of representing a charge transporter.

ground state representation of $\mathfrak{A}$, that is, the cyclic representation π_0 associated to the (unique) translation invariant ground state ω_0 of the toric code, on a Hilbert space $\mathcal{H}$, with ω_0 represented as a unit vector $\Omega \in \mathcal{H}$.

We are interested in ways to create states that Alice and Bob can distinguish, but Eve cannot. Of course, if Alice and Bob have access to both Λ_A and Λ_B, they can just store their information by acting with local operators in one (or both) of the cones, and Eve will not be able to detect this. This scenario in itself is not that interesting, so we ask the question what they can do if they *in addition* have access to operations that are not generated by the local observables in Λ_A or Λ_B, but nevertheless invisible to Eve. Potentially, this gives them more power compared to the 'baseline' scenario of local operations on their cones, and it are these additional capabilities that we want to investigate. The idea is to create a pair of charges, with one end of the pair in each cone. Since we are interested in the *additional* power of Alice and Bob, we can disregard local modifications of these states that can be obtained by acting with observables in $\mathcal{R}_A$ or $\mathcal{R}_B$. Such operations include moving the charge around in the cone, or introducing pairs of charge and conjugate charge within a cone. We will come back to this point after we introduce the main idea in more detail.

Note that the operations that Alice and Bob can perform in their respective cones commute with the observables Eve has at hand. This is the locality condition that is already built into the construction of the systems. We will show that we can use the charge transporters V_X, V_Z and V_Y that create pairs of excitations distributed over the cones Λ_A and Λ_B to construct states that the authorised parts can distinguish. They are unitaries on the Hilbert space $\mathcal{H}$ and one can think of them as creating correlations between the cones when applied to the ground state vector Ω. Even though they are not localised in $\Lambda_A \cup \Lambda_B$, they still commute with all of Eve's observables, and hence are elements of $\widehat{\mathcal{R}}_{AB}$. The reason is that they can be obtained as weak operator limits of path operators. That is, one chooses a site in each cone, and connects them with a path (see figure 7). Then, as n grows, we let the path go to infinity (in the sense that it will avoid any finite subset of Λ_E eventually, keeping the endpoints fixed). The corresponding path operators then converge to the charge transporter in the weak-operator topology. As a result the charge transporters commute with all of Eve's local observables, and hence are contained in $\widehat{\mathcal{R}}_{AB}$ [30]. From this it already follows that if $E \in \mathcal{R}_E$ is any operator on Eve's part of the system, its expectation values in the states $V_X\Omega$, $V_Z\Omega$, $V_Y\Omega$ and Ω coincide. That is, consider for example the state $V_i\Omega$ with $i = X$, Z or Y, then $\langle V_i\Omega, EV_i\Omega\rangle = \langle \Omega, V_i^* E V_i \Omega\rangle$. Since $V_i \in \widehat{\mathcal{R}}_{AB}$ we have $[V_i, E] = 0$, and therefore

$$\langle V_i\Omega, EV_i\Omega\rangle = \langle \Omega, E\Omega\rangle, \quad i = X, Z, Y.$$

Hence Eve cannot distinguish between the states in $\mathcal{C} \coloneqq \{\Omega, V_X\Omega, V_Z\Omega, V_Y\Omega\}$ by acting with local operators on her system. On the other hand Alice and Bob can distinguish these states by acting locally on their cones: the construction of the charge transporters includes a specification of a site in each cone and the transporters create a pair of conjugate excitations from the ground states at these sites. Alice and Bob can now locally measure the flux through a (Wilson) loop around the respective sites to determine which excitation or whether at all was created. In other words, they do a charge measurement in their respective cones. The position of the site inside the cone itself is not so important here (that is why we did not specify it further) since there are always unitaries with support in either of the cones that can move the excitation around.

This means, that Alice and Bob each possess a POVM that allows them to distinguish the states in $\mathcal{C}$. The choice of this POVM is not unique, since it depends on the loops around the site at which the excitation created by V_i is localised. It can in principle be any loop of any size as long it surrounds the excitation. The flux measurement corresponds to a projection on the enclosed area onto the excitation one wants to measure

(detailed descriptions of these projections can be found in [7, 40]). The POVM elements then simply consist of the projections on the different excitations that can occur, given that the loop is fixed.

The above construction can be extended a bit. In the end, Alice and Bob are only interested in the *total* charge in their region. Acting with local operators in either of the cones might move the existing charge around, or create pairs of conjugate charges, but the *total* charge does not change. Hence, instead of just the states $V_i\Omega$, we can consider the four spaces $\mathcal{R}_{AB}V_i\Omega$ (or their closure). To Eve, all these states look the same, since $\mathcal{R}_{AB} \subset \mathcal{R}_E$, but Alice and Bob can in principle distinguish the four subspaces. Note that this is less practical, since the location of the charge of interest is not known, and Alice and Bob have to make sure their charge measurements encompass a big enough region. The projections that measure the *total* charge in Λ_A or Λ_B are both in $\mathcal{R}_{AB}$, but these operations clearly are not local any more. For simplicity, we restrict to the set $\mathcal{C}$ of four states, and ignore the local modifications in the cones: the corresponding statements for that case can be obtained straightforwardly[10].

If we go back to the finite-dimensional description of secret sharing schemes where the Hilbert space is described by a tensor product of n Hilbert spaces, it can be easily checked that for a set $A \subset \{1, \ldots, n\}$ to be authorised with respect to a code space $\mathcal{C}$ is equivalent to requiring the existence of a POVM $\{E_i\}$ acting on $\mathcal{H}_A$ such that $E_i\psi_j = \delta_{i,j}\psi_j$ where $\psi_j \in \mathcal{C}$. It is necessary that the POVM elements commute with the operators acting on the complement of A. It makes sense then to rephrase the condition on A to be authorised to the following: elements E that commute with the observables $\mathfrak{B}(\mathcal{H}_A)$ on A such that it holds that $\langle\psi_i, E\psi_j\rangle = 0$ if $i \neq j$. Note that this is equivalent to the original definition, since the Hilbert space decomposes as a tensor product of the authorised part $\mathcal{H}_A$ and its complement $\mathcal{H}_{A^c}$.

In the infinite dimensional setting we do not necessarily have a decomposition of the Hilbert space into tensor products. But the algebraic view still allows for the characterisation of authorised sets. That is, we say that a subalgebra $\mathcal{N}$ of our system's algebra $\pi_0(\mathfrak{A})''$ is authorised with respect to the classical code space $\mathcal{C}$ if for all $E \in \mathcal{N}'$ and all $\psi_i, \psi_j \in \mathcal{C}$ with $i \neq j$ it holds that $\langle\psi_i, E\psi_j\rangle = 0$.

We can show that in our example of the toric code this is true for both Alice's and Bob's observables $\mathcal{R}_A$ and $\mathcal{R}_B$. In order to prove this it is crucial to understand what the structure of the commutants $\mathcal{R}'_A$ and $\mathcal{R}'_B$ is. In the following we only consider Alice's observables $\mathcal{R}_A$, since the case for Bob can be understood analogously. In fact it was shown [33] that the von Neumann algebra $\mathcal{R}_A$ satisfies *Haag duality*, that is, $\mathcal{R}_A = \mathcal{R}'_{A^c}$. Hence the commutant $\mathcal{R}'_A$ is exactly given by the observables $\mathcal{R}_{BE}$ on the complement $A^c = BE$ of Alice's cone. In the thermodynamic limit, this statement is non-trivial, the reason being that the algebras $\mathcal{R}_{BE}$ and $\mathcal{R}_A$ do not live on different tensor factors of the underlying Hilbert space. Moreover, it is in fact false for the algebra $\mathcal{R}_{AB}$ (in the sense that $\mathcal{R}'_{AB} \neq \mathcal{R}_{AB^c} = \mathcal{R}_E$) of observables localised in both cones Λ_A and Λ_B, which is the whole reason that our construction works. In that case $\mathcal{R}_{AB}$ is properly included in the $\widehat{\mathcal{R}}_{AB}$, which as we recall is the algebra of observables that commute with all of Eve's observables. Hence Haag duality for cone algebras and its failure for the algebra $\mathcal{R}_{AB}$ are important for our setting. Even more, the identification of Alice's and Bob's part of the system, Λ_A and Λ_B, as authorised sets by just the requirement that $\mathcal{C}$ corrects errors on their complements Λ_A^c and Λ_B^c still makes sense.

Now let $\psi, \phi \in \mathcal{C}$ be distinct states and $E \in \mathcal{R}'_A = \mathcal{R}_{BE}$. Without loss of generality we can assume that E is a product of ribbon operators F_B and F_E in $\mathcal{R}_B$ and $\mathcal{R}_E$, since the linear span of products of such forms a strongly dense subalgebra of $\mathcal{R}_{AB}$ [33]. Furthermore, recall that $\psi = V_i\Omega$ and $\phi = V_j\Omega$ for some $i \neq j$, including the possibility that $V_0 = I$. Hence $\langle\psi, E\phi\rangle = \langle\Omega, V_i^*F_EF_BV_j\Omega\rangle$. Recall also that the action of the charge transporters V_k on the ground state Ω create an excitation at some site $s_B \in \Lambda_B$ and its conjugate at some site $s_A \in \Lambda_A$. Thus, in order this scalar product be non-zero, the ribbons to which the operators F_E and F_B correspond, needed to connect the sites s_B and s_A with each other. But this is impossible, since this would require a ribbon in Λ_A starting at s_A and connecting to the boundary in Λ_A, and the corresponding ribbon operator would be in $\mathcal{R}_A$. Hence the product $V_i^*F_EF_BV_j$ creates non-trivial excitations above the ground state when acting on Ω, and it follows $\langle\psi, E\phi\rangle = 0$, since states that contain excitations above the ground state are orthogonal to the latter (see also [41]).

Summarising this, we consider the collection of orthonormal states $\mathcal{C} = \{\Omega, V_X\Omega, V_Z\Omega, V_Y\Omega\}$, or rather the classes of states $\mathcal{R}_{AB}V_i\Omega$ (recall that these are orthogonal spaces). Alice and Bob can distinguish these classes of states by doing charge measurements in the cones Λ_A or Λ_B, hence Λ_A and Λ_B are authorised sets. On the other hand, all states look the same for local measurements in $\Lambda_E = (\Lambda_A \cup \Lambda_B)^c$, hence this can be regarded as an unauthorised set. The key properties used for this characterisation are Haag duality of cone algebras in the ground state representation and the detailed knowledge about the local excitation structure above the ground state.

[10] The choice of taking $\mathcal{C} = \{\Omega, V_X\Omega, V_Z\Omega, V_XV_Z\Omega\}$ from the spaces $\mathcal{R}_{AB}V_i\Omega$ can be interpreted as choosing different implementations of secret sharing schemes with same information to be hidden and same access structure. Additionally Alice and Bob can act locally on the state within their cones without the corresponding other being able to notice.

We would like to stress that this scheme cannot be extended to one for sharing quantum information. Given two different code states ψ_i and ψ_j, $i \neq j$ (or, two states in different classes, in the general setting), we could in principle also prepare the superposition $\psi := \frac{1}{\sqrt{2}}(\psi_i + e^{i\varphi}\psi_j)$, where φ is a fixed complex phase. But we cannot distinguish this superposition from any other of these two states by any *local* operation on Λ_A or Λ_B. To see this, consider a local observable $A \in \mathcal{R}_A$. Then, since A just acts in the cone Λ_A the operator $V_i^* A V_j$, $i \neq j$ creates non-trivial excitations above the ground state, hence $\langle \psi_i, A\psi_j\rangle = 0$, and therefore $\langle \psi, A\psi\rangle = \frac{1}{2}\langle \psi_i, A\psi_i\rangle + \frac{1}{2}\langle \psi_j, A\psi_j\rangle$. So local charge measurements lose information about relative phases in the superposition of code states. That is, the code states obey a superselection rule.

Another question is if there are more states which we can add to the already known code states to increase the amount of information Alice and Bob can share (where, as before, we are only interested in states up to acting with local operators in Λ_A or Λ_B). That is, are there perhaps other operations in $\widehat{\mathcal{R}}_{AB}$ that lead us to a new class of states that can be distinguished with local operations in Λ_A or Λ_B? This turns out not to be the case, which can be understood by the JKL index. The charge transporters which are used to create the code states are such that they commute with all observables at Eve's disposal, but are not localised in either cone. Hence the question whether this set of states is complete translates to the question whether we found all charge transporters, corresponding to charges that we may not have found yet. This question can be answered by computing the value of the JKL index: it turns out that all the observables $\widehat{\mathcal{R}}_{AB}$ that commute with Eve's allowed operations $\mathcal{R}_E$ are precisely generated by those in the cone and the unitary operators V_X, V_Z, V_Y, that is $\widehat{\mathcal{R}}_{AB}$ is generated as a von Neumann algebra by the charge transporters and $\mathcal{R}_{AB}$ [11]. This result follows from two steps: first one proves the general result that the index provides a bound on the number of inequivalent charges (and hence, the number of 'inequivalent' charge transporters). Then one can calculate the index itself, and see that the known charge transporters already saturate this bound. This argument shows that we can regard the JKL index then as the maximal number of code states for a secret sharing scheme of classical information. We come back to this point in more detail in section 5.

There is one other point to discuss: is it really necessary to use the operations in $\widehat{\mathcal{R}}_{AB}$? Indeed, if F_ξ is a path operator between the sites in cone Λ_A and Λ_B, then $V_i\Omega = F_\xi\Omega$. The problem is that Alice and Bob at some point have to apply an operator to store the classical information. If they do this by creating a pair of excitations in one cone, and then move one of the excitations to the other cone, Eve could detect the excitation as it moves through her region. Even if Alice and Bob are able to do this so quickly that Eve has no chance of finding out, there is another method for Eve to detect this. So far we have assumed that Eve does not alter her part of the state. That is, the state we start with is Ω. But nothing prevents Eve from doing any operation on her part of the system. For example, she could create a configuration of charges on her side. If the path operator that Alice and Bob apply to the system crosses one of the paths of Eve's operators, the state will acquire a phase because of the anyonic nature of the excitations, which opens up possibilities of detection. If Alice and Bob use the operations in $\widehat{\mathcal{R}}_{AB}$, this cannot happen, although it should be noted that in a laboratory setting this may not be very practical (or even possible). We briefly comment on this last point below.

4.2. TEE and the irreducible correlation

There exists an interesting interplay between the TEE [5, 6] and the irreducible correlation of the state, which provides the TEE with an operational interpretation as the achievable rate of a certain secret sharing scheme of classical information [12].

The irreducible correlation is a measure of correlations on multipartite quantum systems. More generally, the *k-th irreducible correlation* $C^{(k)}(\rho)$ of a state ρ on an n-partite system quantifies how much correlations are contained in the kth reduced density matrix (RDM) $\rho^{(k)}$ that are not contained in the $(k-1)$-RDM $\rho^{(k-1)}$. It is given by the expression $C^{(k)}(\rho) = S(\tilde{\rho}^{(k)}) - S(\tilde{\rho}^{(k-1)})$, where $\tilde{\rho}^{(l)}$ is the state that maximises $S(\sigma)$ when optimising over all states that have the same l-RDM as ρ. Precise definitions can be found in [12, 42].

Consider now a state ρ of a quantum many body system that satisfies an area law with a 'topological' contribution, i.e. $S(A) = \beta|\partial A| - n_{\partial A}\gamma + \mathcal{O}(|\partial A|^{-1})$ for (large) regions A with some constant $\beta > 0$ and $n_{\partial A}$ being the number of connected components of the boundary of A, and γ the TEE. Assume that the correlation length is finite, i.e. $\rho_{AC} = \rho_A \otimes \rho_C$ for disjoint regions A, C that are far away from each other, and that the conditional mutual information between A and C conditioned on B is zero, i.e. $I(A:C|B) = 0$, if the regions A and C are connected through a third region B such that ABC has no holes. Under these conditions it was shown in [12] that the TEE S_{top} coincides with the 3rd irreducible correlations of the reduced density matrix (RDM) on regions ABC [12]. Here ABC is a partition of the system in a configuration as considered in Kitaev–Preskill [6] and similarly in Brown *et al* [16], or as in the Levin–Wen definition of TEE [5]. Note that, borrowing the notation from the introduction, $S_{\text{top}}^{\text{KP}} = \gamma$ and $S_{\text{top}}^{\text{LW}} = 2\gamma$.

If we consider a finite region ABC as in [5, 6] the 3rd irreducible correlation $C^{(3)}(\rho_{ABC})$ thus characterises the correlation in ρ_{ABC} that are not contained in the RDM of any bipartition of the tripartite system ABC.

Furthermore, in [12] it was shown that then $C^{(3)}(\rho_{ABC})$ carries an operational interpretation in terms of the *maximal rate* r_{ABC} of a certain secret sharing scheme of classical information. To be more precise, regarding ρ_{ABC} as a tripartite state over ABC it holds that $C^{(3)}(\rho_{ABC})$ is equal to the optimal sharing rate r_{ABC} for a secret sharing scheme for classical information that encodes information in ρ_{ABC} such that the information can only be decoded by having access to all three regions[11] A, B and C.

That is, for optimal encoding and decoding channels the number bits that can be encoded is given by r_{ABC}. Now since $C^{(3)}(\rho_{ABC}) = r_{ABC}$ this means that the number of bits that can be encoded using the tripartite correlations of ρ_{ABC} is given by S_{top}. For the case of anyon models where the TEE of the ground state is given by $\gamma = \log \mathcal{D}$ and $\mathcal{D}$ is the total quantum dimension, the number of bits that can be encoded is $\mathcal{D}$ in case of $S_{\text{top}}^{\text{KP}}$ and $\mathcal{D}^2$ in case of $S_{\text{top}}^{\text{LW}}$. Therefore the total quantum dimension determines the maximal amount of information we can encode in ρ_{ABC} by just using the tripartite correlations in this state. The difference between the two settings of [5, 6] is a result of the different topologies in the choice of ABC. Intuitively in the Levin/Wen type of regions there exist operators acting along non-contractible loops that leave the ground state invariant and that contribute to $C^3(\rho_{ABC})$ whereas in the Kitaev/Preskill setting such loops can be contracted.

In the thermodynamic limit of the toric code we have, however, a different geometry of the regions A, B and C, where we identify the regions A and B with the cones Λ_A and Λ_B controlled by Alice and Bob, respectively, and C with Eve's part Λ_E. Also note that in this case we have that ABC comprises the whole system, as opposed to the finite dimensional case, where ABC just needs to be a sufficiently large region. As discussed in the previous sections, in this setting $\mathcal{D}^2$ is the dimension of the code space of a secret sharing scheme for classical information between the algebras over disjoint cones. More precisely, the number of equivalence classes $\mathcal{R}_{AB}V_i\Omega$ of states that differ only by local operators in the respective cones, is given by $\mathcal{D}^2$. The code space is maximal in so far as that the JKL index bounds the number of superselection sectors from above [11], and is equal to $\mathcal{D}^2$. In this sense $\log[\widehat{\mathcal{R}}_{AB} : \mathcal{R}_{AB}] = \log \mathcal{D}^2$ is the optimal sharing rate of that scheme and we regard this as an infinite dimensional analogue of the results obtained in [12]. In the next section this equality is discussed in more detail. In the general case we expect that the index also carries a similar interpretation.

The JKL index can also be related to a relative entropy for the inclusion $\mathcal{R}_{AB} \subset \widehat{\mathcal{R}}_{AB}$ which can be interpreted in terms of a Holevo quantity, giving a bound on how much better we can distinguish states using operations from $\widehat{\mathcal{R}}_{AB}$, compared to with just operations from $\mathcal{R}_{AB}$. The details can also be found in the next section. Consequently the thermodynamic limit exhibits a very similar structure as in the situation of finite lattices.

4.3. Can we work around superselection sectors?

The secret sharing task we described depends on the presence of charge transporters, and hence of superselection sectors. These are modelled as equivalence classes of representations, satisfying the localisation criterion (3). The idea to use superselection sectors to assist in quantum information tasks is not new, see for example [43], where the authors apply the fact that local operators cannot distinguish the different superselection sectors to a data hiding protocol.

It is natural to ask if superselection sectors can be used to circumvent certain no-go theorems in quantum information. Unfortunately, this turns out not to be the case, if we assume an adversary Eve has access to an auxiliary system to store compensating charges [44]. Hence the authors of [44] conclude that superselection sectors cannot be used to increase the security of quantum information protocols.

This result appears to be at odds with our claim that Alice and Bob can share a secret securely with the help of superselection sectors (which is essential in our construction). This is not the case, since the two settings are fundamentally different. In particular, Kitaev *et al* consider the case where the superselection sectors are given by a compact group symmetry. The adversary Eve is then allowed to do *any* operation that commutes with this symmetry. If she has an auxiliary system available in which she can store a compensating charge, she can implement arbitrary transformations without breaking the symmetry. In our setting, we know that the symmetry is not given by a group (since our anyons are describe by a modular tensor category), and Eve does not have an auxiliary system at her disposal. In addition, she can only do *local* operations, which further limits her powers. In particular, such operations cannot interpolate between different superselection sectors, at least not in our setting, where the we describe infinite systems.

We also do not need to assume that the total charge in the system is zero, it is enough to know that the total charge in both Alice's and Bob's cone is trivial, which they can check before starting the secret sharing protocol. If there are only *abelian* sectors, even this assumption is not necessary: Alice and Bob can each measure the total charge in their cone before the protocol starts, and record the result. Since the fusion rules in that case give a *unique* charge after fusing two anyons, they can compensate their measurements by computing the result of

[11] The optimal rate determines how many bits can at most be encoded in the state ρ_{ABC} that it there exists a decoding channel that reliably can recover the information in asymptotic many uses of the scheme.

fusion with the conjugate charge. In the non-abelian case this is no longer true, since there are multiple fusion outcomes.

5. Channels and entropy

The secret sharing task we described suggests a description in terms of quantum channels. In particular, we would like to have a quantum channel that compares the 'full' operations available to Alice and Bob, described by $\widehat{\mathcal{R}}_{AB}$, to the strictly local operations $\mathcal{R}_{AB}$. Fortunately the index theory for subfactors provides such a map. This is the map that we investigate in this section. Moreover, it is possible to define a relative entropy for subfactors. This relative entropy is related to the index of the inclusion. Here we will argue that this relative entropy makes it possible to connect the index to the well-known Holevo χ-quantity, which tells us how well we can distinguish states, and is related to the classical capacity of a quantum channel.

We will again consider the toric code here, although the abstract constructions work for any subfactor with finite index. The toric code however has the advantage of being simple enough to allow a concrete analysis, and at the same time providing a clear physical interpretation. It will allow us to match the mathematical constructions to physical processes.

5.1. Channels

The inclusion $\mathcal{R}_{AB} \subset \widehat{\mathcal{R}}_{AB}$ of the cone observables into the algebra of observables that commute with Eve's observables is accompanied by a *conditional expectation* $\mathcal{E} : \widehat{\mathcal{R}}_{AB} \to \mathcal{R}_{AB}$ [11, 32], that is, a generalisation of the partial trace to the language of operator algebras. A conditional expectation is a (normal) unital completely positive (cp) map such that $\mathcal{E}(ABC) = A\mathcal{E}(B)\,\mathrm{C}$ for all $A,\ C \in \mathcal{R}_{AB}$ and $B \in \widehat{\mathcal{R}}_{AB}$. The subalgebra $\mathcal{R}_{AB}$ hereby plays the role of the subsystem. In fact $\mathcal{E}$ is a channel; it is linear, cp, preserves the identity operator and is normal in the sense that it maps normal states to normal states. These are states that are represented by density matrices on the Hilbert space on which the algebra is represented. As mentioned earlier elements of $\widehat{\mathcal{R}}_{AB}$ can be expressed as linear combination of some 'basis' with coefficients in $\mathcal{R}_{AB}$. Moreover the algebra $\widehat{\mathcal{R}}_{AB}$ is generated as a von Neumann algebra by $\mathcal{R}_{AB}$ and the charge transporters $\{V_X,\ V_Z\}$. With the notation $V_i,\ i = 0, X, Z, Y$ with $V_0 = I$ and $V_Y = V_X V_Z$, the basis expansion of elements $X \in \widehat{\mathcal{R}}_{AB}$ is then $X = \sum_i A_i V_i$ with $A_i \in \mathcal{R}_{AB}$ [11]. Another way of saying this is that $\widehat{\mathcal{R}}_{AB}$ is a left module over $\mathcal{R}_{AB}$. In this case the operators V_i are also called a 'Pimsner–Popa basis'.

The channel $\mathcal{E}$ is then given by

$$\mathcal{E} : \widehat{\mathcal{R}}_{AB} \to \mathcal{R}_{AB} : X \mapsto A_0. \tag{4}$$

In a sense it leaves the states $\Omega,\ V_X\Omega,\ V_Z\Omega$ and $V_Y\Omega$ invariant. This can be seen as follows. In the Schrödinger picture the channel is given by the unique cp map $\mathcal{E}_*$ determined by $\mathcal{E}_*(\rho) := \rho \circ \mathcal{E}$ where ρ is a normal state over $\mathcal{R}_{AB}$. We do not intend to give a full characterisation of $\mathcal{E}_*$ here. Instead we show how it acts the vector states $\Omega,\ V_X\Omega,\ V_Z\Omega$ and $V_Y\Omega$, where Ω is the ground state. Since these are vectors in the Hilbert space, they give rise to normal states on $\mathcal{R}_{AB}$ and on $\widehat{\mathcal{R}}_{AB}$. Let ψ be any of these states and $X \in \widehat{\mathcal{R}}_{AB}$ as above, and let ρ be the corresponding state on $\mathcal{R}_{AB}$. As shown in section 4, $\langle\Omega|\ V_i A V_j\ |\Omega\rangle = 0$ for any $A \in \mathcal{R}_{AB}$ and $V_i \neq V_j$. In particular, this implies that $\langle\psi|\ AV_i\ |\psi\rangle = 0$ if $i \neq 0$, and we find $(\mathcal{E}_*\rho)(X) = \rho(A_0) = \langle\psi|\ A_0\ |\psi\rangle = \langle\psi|\ X\ |\psi\rangle$. Hence the states corresponding to ψ are invariant under the action of $\mathcal{E}_*$. For superpositions this is no longer true since $\mathcal{E}_*$ erases the off-diagonal elements of the density matrices in this basis. Of course the situation is much more complicated for general normal states on $\mathcal{R}_{AB}$ but this illustrates well the classical nature of the secret sharing scheme. Note that the argument still holds if we consider the states $V_i\Omega$, with U a unitary in $\mathcal{R}_{AB}$, so that we again have four classes of (vector) states.

Before we come to the information-theoretical interpretation of the map $\mathcal{E}$, we first make another interesting observation. There is a canonical way to get a tower of inclusions of von Neumann algebras if we have a finite index subfactor. We here give an example of extending the tower downwards. Recall that the charge transporters constitute a unitary representation of the group $\mathbb{Z}_2 \times \mathbb{Z}_2$ on the Hilbert space of the ground state representation. This representation induces an action on the operators by conjugation. This action maps $\mathcal{R}_{AB}$ into itself. Therefore the twirl $\mathcal{E}_1(A) := \frac{1}{4}\sum_i V_i A V_i^*$, $A \in \mathcal{R}_{AB}$ is a conditional expectation from the cone algebra $\mathcal{R}_{AB}$ to the subalgebra $\mathcal{R}_0$ of fixed points of this action. The inclusion $\mathcal{R}_0 \subset \mathcal{R}_{AB}$ then has index $[\widehat{\mathcal{R}}_{AB} : \mathcal{R}_{AB}]$. Furthermore, the channel $\mathcal{E}_1$ is implemented by the projection $P_0 = \frac{1}{4}\sum_i V_i$ in the sense that $\mathcal{E}_1(A)P_0 = P_0 A P_0$. This subalgebra consists of these operations in the cones Λ_A and Λ_B which cannot distinguish the states $\Omega,\ V_X\Omega,\ V_Z\Omega$ and $V_Y\Omega$ from each other. In this sense the channel $\mathcal{E}_1$ can be interpreted as the completely depolarising channel on these states.

5.2. Relative entropies and classical information

The index can be connected to a relative entropy [45]. Here we follow the work of Hiai [46], who discusses the case of general subfactors (not just Type II_1[12]) and gives different characterisations of the index. We start with defining the relative entropy of a pair of von Neumann algebras $\mathfrak{N} \subset \mathfrak{M}$ with respect to a normal state φ on $\mathfrak{M}$. This is given by

$$H_\varphi(\mathfrak{M}|\mathfrak{N}) = \sup_{(\varphi_i)} \sum_i [S(p_i\varphi_i, \varphi) - S(p_i\varphi_i|_{\mathfrak{N}}, \varphi|_{\mathfrak{N}})], \tag{5}$$

where again we use $|$ to denote restriction to a subalgebra. The supremum is over all *finite* convex combinations such that $\varphi = \sum_i p_i\varphi_i$, with φ_i a normal state. That is, we consider all different preparations of the state φ. The relative entropy $S(p_i\varphi_i, \varphi)$ is to be understood in the sense of Araki [47] (see [48] for an introduction). Compared to these references we switched the order of the arguments to agree with the usual definition in quantum information. The definition of Araki reduces to the well-known formula for the quantum relative entropy of finite systems if the algebras are matrix algebras. We also note that the terms in square brackets are positive. This is perhaps not immediately clear, but essentially follows from the monotonicity of the relative entropy (restricting the states is like tracing out a part of the system).

First we find it useful to find a physical interpretation of equation (5). Intuitively, it should capture how well we can distinguish states when we have all operations in $\mathfrak{M}$ at our disposal, compared to when only measurements (or, POVM's) from $\mathfrak{N}$ are allowed. To make this intuition more precise, consider the following scenario which is typical when trying to send classical information over a quantum channel. We largely follow Holevo [49] (but also see [50]), and for the moment consider finite dimensional systems. Let ρ be a state on the system. If ρ is a mixed state, there are different ways to prepare this state. In particular, consider a probability distribution p_x and let ρ_x be states such that $\rho = \sum_x p_x\rho_x$. That is, Alice picks a state according to the probability distribution p_x. The question then is if Alice sends this state to Bob, how well Bob can recover the distribution p_x. In general, even if Alice sends many copies, Bob cannot recover p_x exactly, for example when the ρ_x are pure but overlapping states. How well Bob is able to recover p_x is governed by the Holevo χ-quantity, defined as

$$\chi(\{p_x\}, \{\rho_x\}) \coloneqq S(\rho) - \sum_x p_x S(\rho_x) = \sum_x p_x S(\rho_x, \rho). \tag{6}$$

This is a quantum generalisation of the Shannon information, and gives an upper bound on the amount of information Bob can recover. The equality follows from the definition of the relative entropy.

In the infinite setting that we are interested in, the definition of the entropy $S(\rho)$ is problematic (since it typically scales with the dimension of the system), and it is better to stick to the relative entropy. We therefore take the right-hand side of equation (6) as the definition of χ. Using the identity $S(p_i\varphi_i, \varphi) = p_i S(\varphi_i, \varphi) + p_i \log(p_i)$, we can rewrite equation (5) to

$$H_\varphi(\mathfrak{M}|\mathfrak{N}) = \sup_{(\varphi_i)} \chi(\{p_i\}, \{\varphi_i\}) - \chi(\{p_i\}, \{\varphi_i|_{\mathfrak{N}}\}).$$

By the previous paragraph, this tells us the maximum amount of extra information we can gain if we are allowed to use operations from $\mathfrak{M}$, compared to when only operations from $\mathfrak{N}$ are allowed, in case the state φ is sent. Sometimes it is also called the 'quantum privacy', since it tells us how much information is inaccessible for $\mathfrak{N}$.

We now come back to the inclusion $\mathcal{R}_{AB} \subset \widehat{\mathcal{R}}_{AB}$. The discussion of the secret sharing protocol shows that $\widehat{\mathcal{R}}_{AB}$ contains operators that are not in $\mathcal{R}_{AB}$, that make it possible to share classical information. Conversely, it is possible to discern more states using operations in $\widehat{\mathcal{R}}_{AB}$ compared to $\mathcal{R}_{AB}$. Hence we expect that there are states φ such that $H_\varphi(\widehat{\mathcal{R}}_{AB}|\mathcal{R}_{AB}) > 0$. This is indeed the case. In fact, we will relate these relative entropies to the quantum dimension, by relating it to the JKL index of the inclusion.

To do this, recall that if the subfactor $\mathcal{R}_{AB} \subset \widehat{\mathcal{R}}_{AB}$ has finite index, then there is a conditional expectation $\mathcal{E} : \widehat{\mathcal{R}}_{AB} \to \mathcal{R}_{AB}$ such that there is some $\lambda > 0$ with $\mathcal{E}(X) \geqslant \lambda X$ for all positive operators $X \in \widehat{\mathcal{R}}_{AB}$. In fact, there is a unique conditional expectation $\mathcal{E}$ maximising the constant λ [32]. In the example of the toric code it is the map $\mathcal{E}$ of equation (4). The index is then equal to the inverse of the best such constant, with the convention that the index is infinite if there is no conditional expectation for which such a (positive) λ exists. Conversely, the existence of such a conditional expectation implies that the index is finite, in particular there is a $\lambda > 0$.

Consider then the conditional expectation $\mathcal{E}$ that maximes the bound. One can then define the relative entropy with respect to $\mathcal{E}$ by

$$H_{\mathcal{E}}(\widehat{\mathcal{R}}_{AB}|\mathcal{R}_{AB}) \coloneqq \sup H_\varphi(\widehat{\mathcal{R}}_{AB}|\mathcal{R}_{AB}).$$

[12] Von Neumann algebras which have trivial centres (in other words, factors), can be classified in types I, II_1, II_∞ and Type III. Type I factors are precisely those that are isomorphic to $\mathfrak{B}(\mathcal{H})$ for some Hilbert space $\mathcal{H}$. The type of the factors has important implications for the technical parts of the index theory, but the qualitative features are largely the same.

The supremum is over all faithful normal states φ on $\widehat{\mathcal{R}}_{AB}$ such that $\varphi \circ \mathcal{E} = \varphi$. In general the relative entropy $H_{\mathcal{E}}(\widehat{\mathcal{R}}_{AB}|\mathcal{R}_{AB})$ is bounded from above by the logarithm of the index $[\widehat{\mathcal{R}}_{AB} : \mathcal{R}_{AB}]$ (see below for the argument in the easier Type II_1 case). By corollary 7.2 of [46], however, equality is attained if and only if the conditional expectation $\mathcal{E}$ maximises the bound in the previous paragraph. Hence we have

$$H_{\mathcal{E}}(\widehat{\mathcal{R}}_{AB}|\mathcal{R}_{AB}) = \log[\widehat{\mathcal{R}}_{AB} : \mathcal{R}_{AB}]. \tag{7}$$

This relates the quantum dimension to a quantity that has a clear operational interpretation in terms of the amount of information that can be hidden. As an aside, for such φ one can actually simplify the formula for $H_{\varphi}(\mathfrak{M}|\mathfrak{N})$ a bit:

$$H_{\varphi}(\mathfrak{M}|\mathfrak{N}) = \sup_{(\varphi_i)} \sum_i S(\varphi_i, \varphi_i \circ \mathcal{E}).$$

The optimisation is again over all (finite) decompositions of φ.

To get some intuition for the quantity $H_{\mathcal{E}}(\mathfrak{M}|\mathfrak{N})$ for some inclusion $\mathfrak{N} \subset \mathfrak{M}$ of von Neumann algebras, it is useful to consider the case where $\mathfrak{M}$ and $\mathfrak{N}$ are of Type II_1. It can be shown that this is not true in the case we are interested in [33], but the example is illustrative nonetheless. In the Type II_1 case, there is a (faithful) tracial state τ on $\mathfrak{M}$, that is, a state such that $\tau(AB) = \tau(BA)$. It should be noted that Type II_1 factors are defined on infinite dimensional Hilbert spaces, so that τ is not the familiar trace of bounded (trace class) operators. If the index is finite, a trace preserving conditional expectation $\mathcal{E} : \mathfrak{M} \to \mathfrak{N}$ exists, with the index being equal to the inverse of the best constant λ as above. Note that this further supports the notion of $\mathcal{E}$ as a quantum channel (since in the usual setting they are required to preserve the trace). In that case, it can be shown that the relative entropy can be rewritten as follows, where we set $\lambda_{x_i} \coloneqq \tau(x_i)$ [46]:

$$H_{\mathcal{E}}(\mathfrak{M}|\mathfrak{N}) = \sup_{(x_i)} \sum_i \lambda_{x_i} [S(\mathcal{E}(\rho_{x_i})) - S(\rho_{x_i})]. \tag{8}$$

Here ρ_{x_i} is the density operator x_i/λ_{x_i} and the entropy S is defined with respect to τ. The supremum is over all finite sets of positive operators x_i such that $\sum_i x_i = 1$. In other words, it is an optimisation over all (finite) POVMs. Note that instead of looking at states, we now look at the possible operations we can use to distinguish states. The quantity between square brackets is called the *entropy gain* in [51].

Before we comment on the physical interpretation of equation (8), we come back to the claim on why it is equal to the Jones index. Again, we consider the Type II_1 case for simplicity, following Pimsner and Popa [45]. The case of infinite factors that we need here is technically much more involved, but uses some similar ideas [46]. Recall that there is a $\lambda > 0$ such that $\mathcal{E}(X) \geqslant \lambda X$ for all positive X. Then, since the logarithm is operator increasing, from equation (8) one can show that $H_{\mathcal{E}}(\mathfrak{M}|\mathfrak{N}) \leqslant \log \lambda^{-1}$. Since one of the equivalent definitions of the index is that it is the inverse of the best of such constants λ, it follows that $H_{\mathcal{E}}(\mathfrak{M}|\mathfrak{N}) \leqslant \log[\mathfrak{M} : \mathfrak{N}]$. To complete the argument Pimsner and Popa find lower bounds for $H_{\mathcal{E}}(\mathfrak{M}|\mathfrak{N})$, and show that in the case of irreducible factors (such as we consider here), equality is in fact attained. The proof of this is more involved, and requires properties of subfactors that are out of the scope of this paper.

To understand equation (8) a bit better, note that since $\mathcal{E}(I) = \mathrm{I}$, we can add $S(I) - S(\mathcal{E}(I))$ to the right-hand side of equation (8). But in that case, it simplifies to

$$\sup_{I=\sum \lambda_x \rho_x} \chi(\{\lambda_x\}, \{\rho_x\}) - \chi(\{\lambda_x\}, \{\mathcal{E}(\rho_x)\}).$$

Note that that the optimisation is *only* over ensembles that sum up to the completely mixed state. This should be contrasted with the (Holevo) channel capacity $\chi_{\mathcal{E}} \coloneqq \sup_{\{p_x\},\{\rho_x\}} \chi(\{\lambda_x\}, \{\mathcal{E}(\rho_x)\})$, which gives the amount of classical information that can be transmitted using the channel [52]. Note that here the optimisation is over *all* ensembles.

We also like to point out the similarity to wiretap channels. In a quantum wiretap channel, quantum information is sent form Alice to Bob, with an eavesdropper Eve. Such a channel maps density operators on $\mathcal{H}_A$ into $\mathcal{H}_B \otimes \mathcal{H}_E$ via a map $\rho \mapsto V\rho V^*$, where V is an isometry. Note that any quantum channel can be written in this form by means of a Stinespring dilation. The point of the wiretap channel is that certain information is inherently private, in the sense that no measurement on $\mathcal{H}_E$ can recover it. This was first studied for quantum channels by Schumacher and Westmoreland [53]. Later this analysis was extended, for example by allowing simultaneous use of multiple copies of the channel [54]. This for example leads to a proof that the (classical) private information is bounded from below by the (quantum) channel capacity. Although our setting is slightly different, the definition of what information is inaccessible or private is essentially the same.

There is yet another description of essentially the same problem, in terms of a subfactor that is closer to the protocol outlined earlier. The inclusion $\mathcal{R}_{AB} \subset \widehat{\mathcal{R}}_{AB}$ could be understood by considering the charge transporters. The interpretation above however does not directly connect to the secret sharing scheme described earlier. A property of the index is that it is invariant under taking commutants:

$$[\widehat{\mathcal{R}}_{AB} : \mathcal{R}_{AB}] = [\mathcal{R}'_{AB} : \widehat{\mathcal{R}}'_{AB}].$$

Note that $\widehat{\mathcal{R}}'_{AB} = \pi(\mathfrak{A}(\Lambda_E))''$, that is, the von Neumann algebra generated by all local observables accessible to Eve. In contrast, $\mathcal{R}'_{AB}$ contains *more* operations. In particular, it contains projections that measure the total charge in one of the cones. These projections are not in Eve's algebra, hence she cannot use them. This is precisely what Alice and Bob use to hide information from her, and by a similar analysis as we have provided above, the amount of information that can be hidden in this way is quantified by the index.

5.3. Total quantum dimension

The discussion above gives a relation between the index $[\widehat{\mathcal{R}}_{AB} : \mathcal{R}_{AB}]$ and the amount of inaccessible classical information. In particular, this can be quantified by equation (7), so it would be good to have a better understanding of $[\widehat{\mathcal{R}}_{AB} : \mathcal{R}_{AB}]$. From section 3.2 we see that this number tells us (in a sense) how much bigger $\widehat{\mathcal{R}}_{AB}$ is than $\mathcal{R}_{AB}$, while section 3.3 and the example in section 5.1 indicate that this is related to the superselection sectors (or anyons) of the theory. On the other hand, the TEE is related to the logarithm of the total quantum dimension, while also quantifying achievable rates in a secret sharing scheme, as discussed in section 4.2. Hence it would be reasonable to assume that there is a relation between the index and the total quantum dimension.

This is indeed the case, and can be shown without any reference to any communication protocols. Already in 1989 Longo showed that the quantum dimension d_i of a representative of a superselection sector can be obtained as the index of a certain inclusion of von Neumann algebras [32]. Later in 2001 it was shown that for the class of rational conformal field theories on the circle, the total quantum dimension is equal to the index of an inclusion $\mathcal{R} \subset \widehat{\mathcal{R}}$, very similar to the inclusion $\mathcal{R}_{AB} \subset \widehat{\mathcal{R}}_{AB}$ [55], and indeed our results are partially motivated by that paper.

A similar strategy can be applied to the lattice models that we are interested in. If we assume (in addition to the technical conditions of Haag duality and the approximate split property mentioned above) that each charge has a corresponding conjugate charge (or show that they exist), it is always possible to define the quantum dimension of a charge. In that case, the relation $[\widehat{\mathcal{R}}_{AB} : \mathcal{R}_{AB}] = \sum_i d_i^2$ holds [11, 55], where the sum is over all distinct charges ρ_i, and d_i is the corresponding statistical (quantum) dimension. If we do not assume existence of conjugate charges, the index still gives an upper bound on the number of them.

It should be noted that this is more than abstract theory. For example, for the toric code one can explicitly show that Haag duality and the approximate split property hold [33]. It is also possible to explicitly obtain representatives of different superselection sectors, and for example show that conjugates exist [30]. Finally, independently from the superselection sector analysis, it can be shown that $[\widehat{\mathcal{R}}_{AB} : \mathcal{R}_{AB}] = 4$ [11]. In fact, this result can be used to show that in fact any superselection sector of the model is equivalent to one of the explicit representatives that can be constructed. Hence for the toric code, the whole program can be carried out in full detail, and we see that also using the index method, we see that we can hide four classical bits.

To summarise the discussion, we can conclude that the total quantum dimension gives tells us how much classical information can be hidden, in the setup described above. This provides an alternative interpretation way of thinking about the total quantum dimension. One of the advantages is that the argument is completely rigorous, and independent of any results on the finite dimensional models. In particular, we do not need to assume the relation between the TEE and the total quantum dimension. We also point out that the analysis is not restricted to the topologically ordered quantum spin systems that we have looked at so far. Rather, they can be applied to all models (once one makes appropriate technical assumptions) for which one can do a superselection structure analysis in terms of localised and transportable representations. This in particular applies to rational conformal field theories on the circle in the operator-algebraic approach [55].

6. Private quantum subsystems

We have discussed an operational interpretation of the JKL index in terms of a secret sharing task: the anyonic charges allow Alice and Bob to store (classical) bits which are not available to the adversary Eve. This is reminiscent of the theory of *private quantum codes* or *private subsystems* (see [56] and references therein). We argue that our construction can be interpreted in this way.

Our description is stated in terms of observables, hence it is most natural to use the Heisenberg picture. Therefore in our setting a quantum channel will be a unital cp normal (i.e., continuous with respect to the weak-operator topology) map $\mathcal{E} : \mathfrak{M} \to \mathfrak{N}$ between two von Neumann algebras. Its dual is a normal cp map $\mathcal{E}_* : \mathfrak{N}_* \to \mathfrak{M}_*$, mapping normal states to normal states. Since we are dealing with infinite dimensional von Neumann algebras (and Hilbert spaces) it is necessary to go beyond the setting of [56], and we will use the recent generalisation to von Neumann algebras by Crann *et al* [39]. Let $\mathcal{E} : \mathfrak{M} \to \mathfrak{B}(\mathcal{H})$ be a quantum channel, and P a

projection on the Hilbert space $\mathcal{H}$. Suppose moreover that $\mathcal{N}$ is a von Neumann algebra on $P\mathcal{H}$. Then $\mathfrak{A}$ is called *private* for $\mathcal{E}$ with respect to P if $P\mathcal{E}(\mathfrak{M})P \subset \mathcal{N}'$.

Our setup immediately leads to an example of a private quantum channel. The index theory gives us a normal conditional expectation $\mathcal{E} : \widehat{\mathcal{R}}_{AB} \to \mathcal{R}_{AB}$. Hence in particular, $\mathcal{E}$ is a normal cp map. We can choose $\mathfrak{N} = (\mathcal{R}_A \vee \mathcal{R}_B)' = \mathcal{R}'_{AB}$. Since $\mathcal{R}_A \vee \mathcal{R}_B$ is a von Neumann algebra, and therefore equal to its double commutant, it follows that $\mathfrak{N}' = \mathcal{R}_{AB}$. Hence $\mathfrak{N}$ is private for $\mathcal{E}$ with respect to $P = I$. Note also that $\mathcal{R}_E \subset \mathcal{N}$, that is, Eve's observables are private for $\mathcal{E}$.

One can show that $\mathfrak{N}$ is private for $\mathcal{E}$ if and only if it is correctable (in the sense of [57]) for any complementary channel $\mathcal{E}^c$ of $\mathcal{E}$ [39, theorem 4.7]. That is, there is some channel $\mathcal{R}$ such that $\mathcal{E}^c \circ \mathcal{R} = \mathrm{id}_{\mathfrak{N}}$. Here $\mathcal{E}^c$ is a channel of the form $\mathcal{E}^c(X) = V^*XV$ for all $X \in \pi(\widehat{\mathcal{R}}_{AB})'$, where $(\pi, V, \mathcal{H})$ is a Stinespring triple for the channel $\mathcal{E}$.

Consider again the example of the toric code. In that case we have an explicit description of $\widehat{\mathcal{R}}_{AB}$, which allows us to identify such a Stinespring triple. In particular, we know that $\widehat{\mathcal{R}}_{AB}$ is isomorphic to the crossed product $\mathcal{R}_{AB} \rtimes_\alpha (\mathbb{Z}_2 \times \mathbb{Z}_2)$, where $\alpha_g(A) = V_g A V_g^*$ and $g \mapsto V_g$ is a unitary representation of $\mathbb{Z}_2 \times \mathbb{Z}_2$ obtained by mapping $(1, 0) \mapsto V_X$ and $(0, 1) \mapsto V_Z$ [11]. Concretely, denote $\mathcal{H}$ for the Hilbert space of the GNS representation of the translational invariant ground state of the toric code. Then we can define a representation π of $\widehat{\mathcal{R}}_{AB}$ by sending $\sum_{k=0,X,Y,Z} A_k V_k$ (with $A_k \in \mathcal{R}_{AB}$) to the following operator, acting on $\mathcal{H}_S := \mathcal{H} \oplus \mathcal{H} \oplus \mathcal{H} \oplus \mathcal{H}$:

$$\pi\left(\sum\nolimits_k A_k V_k\right) = \begin{pmatrix} A_0 & A_X V_X & A_Z V_Z & A_Y V_Y \\ A_X V_X & A_0 & A_Y V_Y & A_Z V_Z \\ A_Z V_Z & A_Y V_Y & A_0 & A_X V_X \\ A_Y V_Y & A_Z V_Z & A_X V_X & A_0 \end{pmatrix}.$$

This can be shown to give an isomorphism of $\widehat{\mathcal{R}}_{AB}$ with the crossed product. Now define an isometry $V : \mathcal{H} \to \mathcal{H}_S$ by $V\psi = (\psi, 0, 0, 0)$. Then by a short calculation we check that

$$\mathcal{E}(X) = V^*\pi(X)V, \quad X \in \widehat{\mathcal{R}}_{AB},$$

that is, $(\pi, V, \mathcal{H}_S)$ is a Stinespring triple for $\mathcal{E}$. Note that $\pi(\widehat{\mathcal{R}}_{AB})V\mathcal{H}$ is dense in $\mathcal{H}_S$, hence the Stinespring dilation is minimal. Now consider the map $\mathcal{R} : \mathfrak{N} \to \mathfrak{B}(\mathcal{H}_S)$, defined by $\mathcal{R}(N) = \mathrm{diag}(N, N, N, N)$, which is a normal unital cp map. Then since $\mathfrak{N} = \mathcal{R}'_{AB}$, it is clear from the description of π above that $\mathcal{R}(\mathfrak{N}) \subset \pi(\widehat{\mathcal{R}}_{AB})'$. Moreover, $\mathcal{E}^c \circ \mathcal{R} = \mathrm{id}_{\mathfrak{N}}$, hence $\mathfrak{N}$ is correctable for $\mathcal{E}$ (with respect to the identity projection). Similarly one can see that in this representation the twirl channel $\mathcal{E}_1$ from section 5 is represented as $\mathcal{E}_1(A) = \frac{1}{4}\sum_{g\in G} V^*\pi(V_g A V_g^*)V$, $A \in \mathcal{R}_{AB}$, with $G = \mathbb{Z}_2 \times \mathbb{Z}_2$, and $\pi(\mathcal{R}_0)$ is given by matrices of the form $\mathrm{diag}(A, A, A, A)$ with $A \in \mathcal{R}_0$, where $\mathcal{R}_0$ is the fixed-point algebra as before.

This example can be generalised to the abelian quantum double model in a straightforward way. The non-abelian model is more difficult, since there the symmetry is not described by $G \times \widehat{G}$ any more, and we do not expect to find a similar crossed product structure. However, the general setting of the quantum dimension being related to the Jones index still applies, and we expect a similar correctable subalgebra result to hold with respect to the canonical conditional expectation $\mathcal{E}$ one obtains from the index theory. Moreover, what is interesting is that the index gives us a measure of the amount of classical information that is private for Eve. This suggests that the Jones index might be a useful tool in the study of the capacity of quantum channels. We hope to return to this question in the future.

7. Stability under perturbations

There are a few technical assumptions that we needed to make in our analysis of the systems in the thermodynamic limit. In particular, we assume that the superselection sectors associated to the anyons can be strictly localised in cone regions. Although any topological charge should certainly be localisable in such a region, strict localisation is likely a too strong condition in general. This generalisation is important when considering *perturbations* of the system, which is necessary if one wants to show that the quantum dimension is truly an invariant of a topologically ordered quantum phase.

This can be seen as follows. Because of the topological order condition, we expect that the properties of the anyonic excitations will be the same across the whole phase (indeed, they should be by the very definition of a phase). That is, if we perturb the dynamics of our model (without closing the spectral gap), the perturbed ground state should have the same superselection sectors. However, the selection criterion, equation (3), as we have used it here, will generally no longer hold: in the thermodynamic limit the ground states of the deformed model can be obtained by composing the original ground states with an automorphism α [3]. This automorphism is however not *strictly* local. Rather, α satisfies a Lieb–Robinson type of bound, such that for strictly local A, $\alpha(A)$

can in general only be approximated up to a small (exponentially decreasing) error by a strictly local observable. As a consequence, if π satisfies the selection criterion, it is not guaranteed that $\pi \circ \alpha$ does so too, since we only know unitary equivalence of $\pi$and π_0 for observables *outside* any given cone. However, since α is not strictly local, it does not map cone algebras into cone algebras.

As a result it is necessary to adapt the superselection criterion, and in turn the inclusion of the von Neumann algebras associated to the two cones. It should be noted that a similar phenomenon also appears in [12]: their results are only strict in the case of zero correlation length. In either case it is expected that in the thermodynamic limit (or in the operator-algebraic case we are interested in, the limit of growing cone size) the small corrections vanish. We believe the information theoretic interpretation here will be of use in studying this question: for example, instead of correctable algebras in the previous section, one should use ε-correctable algebras [39], which allow for (arbitrarily small) errors in the correction. We hope to come back to this issue in future work.

8. Summary and discussion

We have reviewed the total quantum dimension of topologically ordered systems, in particular how in the thermodynamic limit it can be obtained as the JKL index of an inclusion of certain algebras of observables. It has been argued by other authors [5, 6] that the quantum dimension can also be obtained via TEE in finite dimensional systems, a fundamentally different approach. Nevertheless, it turns out that both quantities have an interpretation in terms of a secret sharing scheme, although the implementation details are different in both cases. Even though our secret sharing scheme is not very practical (and is not intended as such), it provides new insight to the quantum dimension, and gives a completely different viewpoint (or approach) of what appears to be same underlying concept. We believe that this may be beneficial to gaining a better understanding of such systems.

The operator-algebraic approach we advocate here provides a rigorous and elegant mathematical framework. It also has other advantages. For example, inclusions of subfactors are well studied, in particular in the context of the JKL index, and many mathematical results are available. This puts the theory on firm mathematical footing. Moreover, a lot of structure comes for free with a finite index inclusion: we mentioned the conditional expectation $\mathcal{E}$, which can be interpreted as a quantum channel.

We also believe this operator-algebraic approach might be beneficial in the important question of stability of topological phases. Although we have only explicitly mentioned the toric code as a test case, we argued that these structures hold more general in topologically ordered models (with the caveat mentioned in the previous section). Generalisation to the abelian quantum double is straightforward, but also in non-abelian models we expect to have a similar structure. An explicit verification, however, will of course be much more involved. Finally, while we mainly have studied what is usually referred to as 'long-range entangled' phases, an algebraic approach to symmetry protected phases appears to be reasonable; as a toy model one can consider the Kitaev wire, and divide the system into three parts, as we did in the example of the Fibonacci chain. We conjecture that this can be related to a notion of entanglement entropy for symmetry protected phases, see [58].

Although the setting we discussed here is tied to the setting of charges belonging to different superselection sectors, the conditional expectation (and hence a quantum channel) always exists for subfactors of finite index. Moreover, the index is related to a relative entropy, which opens up connections to quantum information theory: the discussion in section 5 is an example of that. We believe that the index theory may be useful to study, for example, capacities of quantum channels, in particular for systems with infinitely many degrees of freedom. Except for the case of gaussian states, there are comparatively few tools available to deal with such examples.

Acknowledgments

TJO was supported by the ERC grants QFTCMPS and SIQS, and by the cluster of excellence EXC201 Quantum Engineering and Space-Time Research. PN has received funding from the European Union's Horizon 2020 research and innovation program under the Marie Sklodowska-Curie grant agreement No 657004. LF is supported by the European Research Council (ERC) through the Discrete Quantum Simulator (DQSIM) project. Many thanks go to K Abdelkhalek, C Bény, C Brell, D Reeb, R Schwonnek and R F Werner for plenty of insightful discussions. The publication of this article was funded by the Open Access Fund of the Leibniz Universität Hannover.

Appendix. Operator algebras

Dealing with quantum systems with infinitely many degrees of freedom, such as the thermodynamic limit of the quantum spin systems we are interested in here, introduces complications that are not present when discussing finite dimensional systems. We prefer to use an operator-algebraic approach to tackle these. In this appendix we give some reasons for why we elect this perspective, and introduce the main definitions and concepts.

To see an example of the difficulties that arise, consider an infinite chain of qubits. Naively, one might expect that the Hilbert space of this system is given by $\mathcal{H} = \bigotimes_{n=-\infty}^{\infty} \mathbb{C}^2$. There is however a problem with the definition of the inner product: let $\psi, \eta \in \mathcal{H}$. Then the inner product should be defined as

$$\langle \psi, \eta \rangle_{\mathcal{H}} := \prod_{n=-\infty}^{\infty} \langle \psi_n, \eta_n \rangle_{\mathbb{C}^2},$$

analogously to the tensor product of a finite number of Hilbert spaces. The problem is that the expression on the right generally does not converge, since it is an infinite product. A simple example is given by taking a unit vector $\Omega \in \mathbb{C}^2$ and setting $\psi_n = \Omega$ and $\eta_n = (-1)^n \Omega$.

We can work around this by using von Neumann's construction of the infinite tensor product: we choose a reference unit vector Ω_n for each n, and only consider vectors $\psi \in \mathcal{H}$ for which $\psi_n \neq \Omega_n$ for only finitely many n. For such vectors the expression above converges and defines an inner product. By taking the completion with respect to the norm obtained from this inner product, we arrive at a Hilbert space $\mathcal{H}$.

This definition is somewhat undesirable, since it depends on the choice of reference vector, and a canonical choice may or may not be available (and results might depend on the choice of vector). In addition, it is not entirely clear what the observables are. One could consider all bounded operators $\mathfrak{B}(\mathcal{H})$ as in single-particle quantum mechanics (potentially considering unbounded observables as well), but this has the downside that one loses some of the locality structure that the chain clearly has. These are some of the reasons why we prefer to work in an operator-algebraic (or, if one wishes, observable-centric) approach, which does not have these problems. For the benefit of the reader we recall the main definitions and explain how they can be interpreted in the context of quantum mechanics (see also [28, 29, 59]).

A.1. C^*-algebras

We want to consider quantum spin systems with infinitely many sites. For concreteness, consider the square lattice $\mathbb{Z}^2$, where at each site there is a quantum spin, with Hilbert space $\mathbb{C}^d$. As remarked above, we cannot just take the infinite tensor product of $\mathbb{C}^d$, and we will focus on the local observables of the system.

Let $\Lambda \subset \mathbb{Z}^2$ be a *finite* subset, consisting of $|\Lambda|$ spins. Since this is a finite quantum spin system, it is described by a Hilbert space $\mathcal{H}_\Lambda = \bigotimes_{x\in\Lambda} \mathbb{C}^d$. Hence the associated observables are the (self-adjoint) elements of

$$\mathfrak{A}(\Lambda) := \mathfrak{B}(\mathcal{H}_\Lambda) = \bigotimes_{x\in\Lambda} M_d(\mathbb{C}).$$

We will find it convenient to call $\mathfrak{A}(\Lambda)$ the *local observables* with support in Λ (or *localised* in Λ), even for those elements that are not self-adjoint.

Now suppose that $\Lambda_1 \subset \Lambda_2$ are both finite subsets of $\mathbb{Z}^2$. Then $\mathcal{H}_{\Lambda_2} \simeq \mathcal{H}_{\Lambda_1} \otimes \mathcal{H}_{\Lambda_2\setminus\Lambda_1}$. Hence we can identify $A \in \mathfrak{A}(\Lambda_1)$ with $A \otimes I_{\mathcal{H}_{\Lambda_2\setminus\Lambda_1}}$ in $\mathfrak{A}(\Lambda_2)$. In addition, if $A \in \mathfrak{A}(\Lambda_1)$ and $B \in \mathfrak{A}(\Lambda_2)$, with $\Lambda_1 \cap \Lambda_2 = \varnothing$ and both finite, it is clear that $[A, B] = 0$. This is known as *locality*, and hence we have a local structure. We want to consider the algebra generated by all such local observables. To this end, define the *(strictly) local observables* by $\mathfrak{A}_{\mathrm{loc}} = \bigcup_\Lambda \mathfrak{A}(\Lambda)$, where the union is over all finite subsets of $\mathbb{Z}_2$, and we identify those operators that come from inclusions $\mathfrak{A}(\Lambda_1) \subset \mathfrak{A}(\Lambda_2)$ in the obvious way.

The algebra $\mathfrak{A}_{loc}$ has a natural norm, induced by the operator norm on $M_d(\mathbb{C})$. It is however not complete with respect to this norm: there are Cauchy sequences in $\mathfrak{A}_{\mathrm{loc}}$ that do not converge. This can be solved by taking the closure with respect to this norm, i.e., by adding limits of Cauchy sequences. This gives a complete normed *-algebra $\mathfrak{A}$, whose norm satisfies $\|A^*A\| = \|A\|^2$ for all $A \in \mathfrak{A}$. Such an algebra is called a C^*–algebra. We call the elements of $\mathfrak{A}$ *quasi-local observables*, since they can be approximated arbitrarily well (in the operator norm) by strictly local observables.

In this setting states are given by positive linear functionals ω of norm one on $\mathfrak{A}$. That is, linear maps $\omega : \mathfrak{A} \to \mathbb{C}$ such that $\omega(A^*A) \geqslant 0$ and $\omega(I) = 1$ (or, equivalently, $\|\omega\| = 1$). The value $\omega(A)$ for a positive operator A has the same interpretation as in Hilbert space quantum mechanics: it is the expectation value of A. We note that states are not necessarily of the form $\mathrm{Tr}(\rho A)$ for some density matrix ρ.

Finally, once we have the algebra of observables we can specify the dynamics by specifying local Hamiltonians. These Hamiltonians generate, under suitable conditions (e.g., the interactions should decay fast enough), a time evolution on the algebra, which is most conveniently described as a one-parameter group $t \mapsto \alpha_t$ of automorphisms. That is, this gives a time evolution of the observables in the Heisenberg picture. Once dynamics are defined it is possible to talk about ground states: these are essentially the states that minimise the

energy. In our case we are usually interested in translationally invariant ground states, and in many of the models of interest they are in addition frustration free: they minimise the expectation values of each local Hamiltonians individually.

The Hilbert space picture can be very useful, and fortunately it is not lost in this algebraic approach. Indeed, the Gel'fand–Naimark–Segal (GNS) construction gives a representation of $\mathfrak{A}$ on a Hilbert space. More precisely, suppose that ω is a state on $\mathfrak{A}$. Then the GNS construction gives a triple $(\pi, \Omega, \mathcal{H})$, where $\mathcal{H}$ is a Hilbert space, π is a representation of $\mathfrak{A}$ as bounded operators on $\mathcal{H}$, that is, a linear map $\pi : \mathfrak{A} \to \mathfrak{B}(\mathcal{H})$ that is compatible with the product and adjoint operation of $\mathfrak{A}$. The state ω is implemented in the Hilbert space by $\Omega \in \mathcal{H}$, in the sense that $\omega(A) = \langle \Omega, \pi(A)\Omega \rangle$ for all $A \in \mathfrak{A}$. Note that this does *not* imply that ω is a pure state. In fact, this is true if and only if π acts irreducibly on $\mathcal{H}$, or equivalently, only multiples of the identity commute with every $\pi(A)$.

A.2. Von Neumann algebras

Now consider a Hilbert space $\mathcal{H}$. Then $\mathfrak{B}(\mathcal{H})$, the algebra of bounded operators on $\mathcal{H}$, is a C^*-algebra. Besides convergence in the operator norm, the underlying Hilbert space gives additional notions of convergence. If $A_i \in \mathfrak{B}(\mathcal{H})$ (or more generally, a net A_λ of operators) is a sequence of operators, we say it converges *strongly*, or in the *strong operator topology*, to an operator $A \in \mathfrak{B}(\mathcal{H})$ if for any $\psi \in \mathcal{H}$, we have that $\|(A_i - A)\psi\| \to 0$. In other words, when acting on a *fixed* vector, we get a convergent sequence. In general the rate of convergence depends on the vector ψ, and if $\mathcal{H}$ is infinite dimensional one cannot conclude that $A_i \to A$ in the operator norm.

There is another topology that has a clear physical interpretation. We say that a sequence A_n of operators converges in the *weak operator topology* to some operator A if for each $\psi \in \mathcal{H}$, we have that $|\langle \psi, A_n\psi \rangle - \langle \psi, A\psi \rangle| \to 0$ if $n \to \infty$. That is, a sequence of observables converges in this topology if we cannot distinguish them (in the limit $n \to \infty$) by measuring in arbitrary vector states.

Now consider a unital *-subalgebra $\mathfrak{M} \subset \mathfrak{B}(\mathcal{H})$. We say that $\mathfrak{M}$ is a *von Neumann algebra* if it is closed in the weak operator topology. This is equivalent to being closed in the strong operator topology, since one can show that both topologies coincide on bounded sets. A perhaps more surprising (and very useful) fact is that this is equivalent to the algebraic condition $\mathfrak{M} = \mathfrak{M}''$, where $\mathfrak{M}' := (\mathfrak{M}')'$, and the prime denotes the commutant in $\mathfrak{B}(\mathcal{H})$. That is, $\mathfrak{M}' := \{T \in \mathfrak{B}(\mathcal{H}) : TX = XT \text{ for all } X \in \mathfrak{M}\}$. This is known as the *bicommutant theorem*. It is easy to check that $\mathfrak{M}''' = \mathfrak{M}'$ if $\mathfrak{M}$ is closed under the *-operation, hence this gives an easy way to obtain von Neumann algebras from subsets of $\mathfrak{B}(\mathcal{H})$.

Finally we would like to mention another useful property of von Neumann algebras, which is not true for general C^*-algebras: they are generated by their projections. This has the following application. Suppose that $O \in \mathfrak{M}$ is some self-adjoint observable that we would want to measure. It is often the case that we cannot (or do not want) the whole observable O, for example due to limitations on equipment, but are content with the following question: does the measured value of O lie in some interval $I = [a, b]$? This yes/no question corresponds to measuring a projection $P_{[a,b]}$. Indeed, it is the spectral projection of O on the interval I. It follows from spectral theory that this projection also is in $\mathfrak{M}$, and hence an observable. This is even true for positive unbounded operators, such as the Hamiltonian H of the system, under mild additional assumptions (in particular, it should be *affiliated* with $\mathfrak{M}$ [28, lemma 2.5.8]). These properties make it natural to look at von Neumann algebras.

References

[1] Chen X, Gu Z-C and Wen X-G 2010 Local unitary transformation, long-range quantum entanglement, wave function renormalization, and topological order *Phys. Rev.* B **82** 155138
[2] Hastings M B and Wen X-G 2005 Quasiadiabatic continuation of quantum states: the stability of topological ground-state degeneracy and emergent gauge invariance *Phys. Rev.* B **72** 045141
[3] Bachmann S, Michalakis S, Nachtergaele B and Sims R 2012 Automorphic equivalence within gapped phases of quantum lattice systems *Commun. Math. Phys.* **309** 835–71
[4] Bravyi S, Hastings M and Michalakis S 2010 Topological quantum order: stability under local perturbations *J. Math. Phys.* **51** 093512
[5] Bravyi S and Hastings M B 2011 A short proof of stability of topological order under local perturbations *Commun. Math. Phys.* **307** 609–27
Levin M and Wen X-G 2006 Detecting topological order in a ground state wave function *Phys. Rev. Lett.* **96** 110405
[6] Kitaev A and Preskill J 2006 Topological entanglement entropy *Phys. Rev. Lett.* **96** 110404
[7] Kitaev A 2003 Fault-tolerant quantum computation by anyons *Ann. Phys.* **303** 2–30
[8] Levin M A and Wen X-G 2005 String-net condensation: a physical mechanism for topological phases *Phys. Rev.* B **71** 045110
[9] Preskill J 1999 *Quantum Computation* (*Lecture Notes for Physics* vol 219) http://theory.caltech.edu/people/preskill/ph219/
[10] Rowell E C and Wang Z 2016 Degeneracy and non-abelian statistics *Phys. Rev.* A **93** 030102
[11] Naaijkens P 2013 Kosaki–Longo index and classifcation of charges in 2d quantum spin models *J. Math. Phys.* **54** 081901
[12] Kato K, Furrer F and Murao M 2016 Information-theoretical analysis of topological entanglement entropy and multipartite correlations *Phys. Rev.* A **93** 022317

[13] Kitaev A 2006 Anyons in an exactly solved model and beyond *Ann. Phys.* **321** 2–111
Wang Z 2010 *Topological Quantum Computation* vol 112 (*CBMS Regional Conference Series in Mathematics*) (Washington, DC: CBMS) pp xiv+115
[14] Wen X-G and Niu Q 1990 Ground-state degeneracy of the fractional quantum Hall states in the presence of a random potential and on high-genus Riemann surfaces *Phys. Rev.* B **41** 9377–96
Hu Y, Stirling S D and Wu Y-S 2012 Ground-state degeneracy in the levin-wen model for topological phases *Phys. Rev.* B **85** 075107
[15] Müger M 2003 From subfactors to categories and topology: I. Frobenius algebras in and Morita equivalence of tensor categories *J. Pure Appl. Algebra* **180** 81–157
[16] Isakov S V, Hastings M B and Melko R G 2011 Topological entanglement entropy of a Bose–Hubbard spin liquid *Nat. Phys.* **7** 772–5
Castelnovo C and Chamon C 2007 Entanglement and topological entropy of the toric code at finite temperature *Phys. Rev.* B **76** 184442
Brown B J, Bartlett S D, Doherty A C and Barrett S D 2013 Topological entanglement entropy with a twist *Phys. Rev. Lett.* **111** 220402
[17] Grover T, Turner A M and Vishwanath A 2011 Entanglement entropy of gapped phases and topological order in three dimensions *Phys. Rev.* B **84** 195120
[18] Huang C-Yu, Chen X and Lin F-Li 2013 Symmetry-protected quantum state renormalization *Phys. Rev.* B **88** 205124
[19] Kim I H 2012 Perturbative analysis of topological entanglement entropy from conditional independence *Phys. Rev.* B **86** 245116
[20] Zou L and Haah J 2016 Spurious long-range entanglement and replica correlation length *Phys. Rev.* B **94** 075151
[21] Shamir A 1979 How to share a secret *Commun. ACM* **22** 612–3
Blakley G R 1979 Safeguarding cryptographic keys *Proc. 1979 AFIPS National Computer Conf.* (Los Alamitos, CA, USA: IEEE Computer Society) pp 313–7
[22] Cleve R, Gottesman D and Lo H-K 1999 How to share a quantum secret *Phys. Rev. Lett.* **83** 648–51
[23] Gottesman D 2000 Theory of quantum secret sharing *Phys. Rev.* A **61** 042311
Kretschmann D, Kribs D W and Spekkens R W 2008 Complementarity of private and correctable subsystems in quantum cryptography and error correction *Phys. Rev.* A **78** 032330
[24] Knill E and Laflamme R 1997 Theory of quantum error-correcting codes *Phys. Rev.* A **55** 900–11
Knill E, Laflamme R and Viola L 2000 Theory of quantum error correction for general noise *Phys. Rev. Lett.* **84** 2525–8
Nielsen M A, Caves C M, Schumacher B and Barnum H 1998 Information-theoretic approach to quantum error correction and reversible measurement *Proc. R. Soc.* A **454** 277–304
Gottesman D 2010 An introduction to quantum error correction and fault-tolerant quantum computation *Quantum Information Science and Its Contributions to Mathematics* (*Proceedings of Symposia in Applied Mathematics* vol 68) ed S J Lomonaco Jr (Providence, RI: American Mathematical Society) pp 13–58
[25] Haah J 2014 An invariant of topologically ordered states under local unitary transformations *Commun. Math. Phys.* **342** 771–801
[26] Pfeifer R N C 2014 Measures of entanglement in non-Abelian anyonic systems *Phys. Rev.* B **89** 035105
Kato K, Furrer F and Murao M 2014 Information-theoretical formulation of anyonic entanglement *Phys. Rev.* A **90** 062325
[27] Trebst S, Troyer M, Wang Z and Ludwig A W W 2009 A short introduction to Fibonacci anyon models *Prog. Theor. Phys. Suppl.* **176** 384
[28] Bratteli O and Robinson D W 1987 Operator algebras and quantum statistical mechanics I. *Texts and Monographs in Physics* 2nd edn (New York: Springer) pp xiv+519
[29] Bratteli O and Robinson D W 1997 Operator algebras and quantum statistical mechanics II. *Texts and Monographs in Physics* 2nd edn (Berlin: Springer) pp xiv+519
[30] Naaijkens P 2011 Localized endomorphisms in Kitaev's toric code on the plane *Rev. Math. Phys.* **23** 347–73
[31] Jones V F R 1983 Index for subfactors *Invent. Math.* **72** 1–25
[32] Kosaki H 1986 Extension of Jones' theory on index to arbitrary factors *J. Funct. Anal.* **66** 123–40
Longo R 1989 Index of subfactors and statistics of quantum fields: I. *Commun. Math. Phys.* **126** 217–47
[33] Naaijkens P 2012 Haag duality and the distal split property for cones in the toric code *Lett. Math. Phys.* **101** 341–54
[34] Fiedler L and Naaijkens P 2015 Haag duality for Kitaev's quantum double model for abelian groups *Rev. Math. Phys.* **27** 1550021
[35] Doplicher S and Longo R 1984 Standard and split inclusions of von Neumann algebras *Invent. Math.* **75** 493–536
Longo R 1984 Solution of the factorial Stone-Weierstrass conjecture: an application of the theory of standard split W^*-inclusions *Invent. Math.* **76** 145–55
[36] Werner R 1987 Local preparability of states and the split property in quantum field theory *Lett. Math. Phys.* **13** 325–9
Summers S J 1996 Bell's inequalities and algebraic structure arXiv:funct-an/9701003
[37] Haag R 1996 *Local Quantum Physics: Fields, Particles, Algebras* 2nd edn (Berlin: Springer) pp xiv+390
[38] Kribs D W, Laflamme R, Poulin D and Lesosky M 2006 Operator quantum error correction *Quantum Inf. Comput.* **6** 382–99
Bény C, Kempf A and Kribs D W 2007 Quantum error correction of observables *Phys. Rev.* A **76** 042303
[39] Crann J, Kribs D W, Levene R H and Todorov I G 2016 Private algebras in quantum information and infinite-dimensional complementarity *J. Math. Phys.* **57** 015208
[40] Bombin H and Martin-Delgado M A 2008 Family of non-Abelian Kitaev models on a lattice: topological condensation and confinement *Phys. Rev.* B **78** 115421
[41] Beigi S, Shor P W and Whalen D 2011 The quantum double model with boundary: condensations and symmetries *Commun. Math. Phys.* **306** 663–94
[42] Zhou D and You Li 2007 Characterizing the complete hierarchy of correlations in an n-party system arXiv:quant-ph/0701029
[43] Verstraete F and Cirac I 2003 Quantum nonlocality in the presence of superselection rules and data hiding protocols *Phys. Rev. Lett.* **91** 010404
[44] Kitaev A, Mayers D and Preskill J 2004 Superselection rules and quantum protocols *Phys. Rev.* A **69** 052326
[45] Pimsner M and Popa S 1986 Entropy and index for subfactors *Ann. Sci. École Norm. Sup.* **19** 57–106
[46] Hiai F 1991 Minimum index for subfactors and entropy II. *J. Math. Soc. Japan* **43** 347–79
Hiai F 1990 Minimum index for subfactors and entropy *J. Operator Theory* **24** 301–36
[47] Araki H 1975/76 Relative entropy of states of von Neumann algebras *Publ. Res. Inst. Math. Sci.* **11** 809–33
Araki H 1977/78 Relative entropy for states of von Neumann algebras II. *Publ. Res. Inst. Math. Sci.* **13** 173–92
[48] Ohya M and Petz D 1993 Quantum entropy and its use *Texts and Monographs in Physics* (Berlin: Springer) pp viii+335
[49] Holevo A S 2012 *Quantum Systems, Channels, Information* (*De Gruyter Studies in Mathematical Physics* vol 16) (Berlin: De Gruyter) pp xiv+349
[50] Wilde M M 2013 *Quantum Information Theory* (Cambridge: Cambridge University Press) pp xvi+655
[51] Holevo A S 2011 Entropy gain and the Choi–Jamiolkowski correspondence for infinite-dimensional quantum evolutions *Theor. Math. Phys.* **166** 123–38

[52] Holevo A S 1979 Capacity of a quantum communications channel *Probl. Inform. Transm.* **15** 247–53
Holevo A S 1998 The capacity of the quantum channel with general signal states *IEEE Trans. Inform. Theory* **44** 269–73
[53] Schumacher B and Westmoreland M D 1998 Quantum privacy and quantum coherence *Phys. Rev. Lett.* **80** 5695–7
[54] Cai N, Winter A and Yeung R W 2004 Quantum privacy and quantum wiretap channels *Probl. Inf. Trans.* **40** 318–36
Devetak I 2005 The private classical capacity and quantum capacity of a quantum channel *IEEE Trans. Inf. Theory* **51** 44–55
[55] Kawahigashi Y, Longo R and Müger M 2017 Multi-interval subfactors and modularity of representations in conformal field theory *Phys. Rev.* B **95** 045111
[56] Jochym-O'Connor T, Kribs D W, Laflamme R and Plosker S 2014 Quantum subsystems: exploring the complementarity of quantum privacy and error correction *Phys. Rev.* A **90** 032305
[57] Bény C, Kempf A and Kribs D W 2009 Quantum error correction on infinite-dimensional Hilbert spaces *J. Math. Phys.* **50** 062108
[58] Marvian I 2013 Symmetry protected topological entanglement arXiv:1307.6617
[59] Keyl M, Schlingemann D and Werner R F 2017 *Phys. Rev.* B **95** 045111
[60] Slofstra W 2016 Tsirelson's problem and an embedding theorem Tsirelson's for groups arising from non-local games arXiv:1606.03140