Quantum Communication in Rindler Spacetime

Kamil Brádler[1], Patrick Hayden[1,2], and Prakash Panangaden[1]

[1]School of Computer Science, McGill University, Montreal, Quebec, Canada
[2]Perimeter Institute for Theoretical Physics, Waterloo, Ontario, Canada

18 September 2011

Abstract

A state that an inertial observer in Minkowski space perceives to be the vacuum will appear to an accelerating observer to be a thermal bath of radiation. We study the impact of this Davies-Fulling-Unruh noise on communication, particularly quantum communication from an inertial sender to an accelerating observer and private communication between two inertial observers in the presence of an accelerating eavesdropper. In both cases, we establish compact, tractable formulas for the associated communication capacities assuming encodings that allow a single excitation in one of a fixed number of modes per use of the communications channel. Our contributions include a rigorous presentation of the general theory of the private quantum capacity as well as a detailed analysis of the structure of these channels, including their group-theoretic properties and a proof that they are conjugate degradable. Connections between the Unruh channel and optical amplifiers are also discussed.

1 Introduction

A well-known feature of quantum field theory in curved spacetimes is the creation of particles from a vacuum [40], which points to a fundamental ambiguity: the notion of particle is not an absolute one in the absence of Poincaré invariance. Even in flat spacetimes one has the Davies-Fulling-Unruh effect [25, 19, 45, 46] whereby a uniformly accelerating observer in Minkowski space detects a thermal bath of radiation in a state that an inertial observer perceives as a vacuum. This phenomenon is symptomatic of a nonuniqueness in the definition of the vacuum state of quantum field theory in curved spacetimes in the absence of some canonical symmetry consideration that allows one to choose a preferred vacuum state.

In quantum information theory, on the other hand, one typically treats the notion of particle as canonical and concepts like "pure state" and "mixed state" are taken to have absolute meaning. In the present work, we examine the consequences for quantum information theory of this ambiguity in the definition of vacuum (and particle) states.

Specifically, we study optimal communications strategies in the face of these relativistic difficulties, building on earlier studies of how relativistic effects impact entanglement manipulation and quantum communications strategies [3, 41, 27, 12, 22, 24, 18, 37]. While most such work studied the degradation caused when protocols not designed for relativistic situations are employed in situations where relativistic effects are significant, our approach will be to design protocols specifically with relativistic effects in mind, in the spirit of [33, 17, 9, 15].

We focus on two scenarios. In the first, an inertial observer, Alice, attempts to send quantum information to an accelerating receiver, Bob, by physically transmitting scalar "photons" of chosen modes. Owing to the thermal noise perceived by the receiver, quantum error correcting codes are required to protect the quantum information.

The second scenario is more elaborate. Two inertial observers – again call them Alice and Bob – communicate by exchanging scalar "photons" of chosen modes, while an accelerating observer – traditionally called Eve – attempts to eavesdrop or wiretap their communication channel. This time, it is Eve who detects thermal noise and therefore cannot perfectly decode the communications between Alice and Bob, thus allowing the possibility of private communication between them. Of course, we are not proposing this as a practical scheme for cryptography but, rather, as an exploration of the impact of relativistic quantum field theory on quantum information theory.

The concept of private capacity in the classical setting is due to Maurer [38] and independently Ahlswede and Csiszar [1]. The private capacity of a quantum channel was first studied by Cai *et al.* and Devetak [13, 20]. These capacities measure the optimal rate at which Alice can transmit classical bits to Bob that remain secret from Eve, in the limit of many uses of the channel. In the present paper we introduce the private *quantum* capacity of a quantum channel, which measures the usefulness of the channel for sending private quantum mechanical data (qubits) instead of bits.

The standard approach to quantum field theory in flat spacetime is to decompose the field into "positive" and "negative" frequency modes as defined by the Fourier transform. One then defines creation and annihilation operators that correspond to these modes and the vacuum state is defined to be the state killed by all the annihilation operators. The Poincaré invariance of Minkowski spacetimes means that the vacuum state is the unique state that is invariant under the action of the Poincaré group. In Rindler space, it is natural for the accelerating observer to use his or her own timelike Killing field to define the notion of positive and negative frequency. This means that there will be a mismatch between Alice's notion of vacuum state and that of the accelerating observer. The transformation between the creation and annihilation operators of the different (and inequivalent) quantum field theories is given by a linear map, called a *Bogoliubov transformation*, between the creation and annihilation operators of the two quantum field theories.

The explicit form of the Bogoliubov transformation is well known and we use it to define a *channel* which we call the Unruh channel. In quantum information theory, a channel is simply any physically realizable transformation of a quantum state. The idea is that the process of transmission may introduce noise and loss of information. Thus,

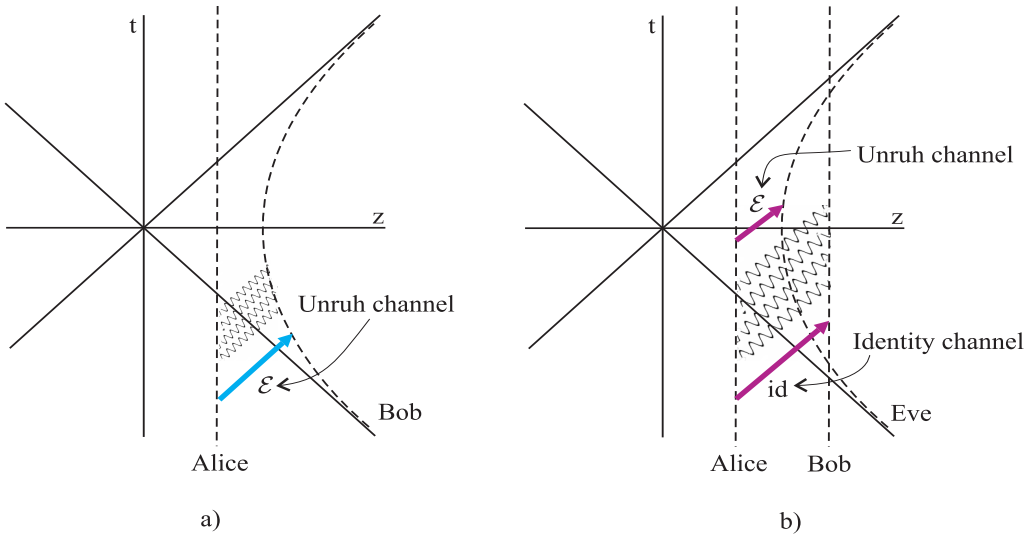

Figure 1: Spacetime diagrams for the two communication scenarios. (a) Alice is an inertial observer try to send quantum information to the uniformly accelerated Bob. The wavy lines indicate transmission via wave packets and the d-rail qudit encoding. (b) In the second diagram, Alice and the intended receiver, Bob, are both inertial observers. In our idealized scenario, they are assumed to share a noiseless quantum channel. A uniformly accelerated eavesdropper, Eve, attempts to wiretap Alice's message to Bob.

an initially pure quantum state may become mixed.

In the Unruh channel, Alice prepares some state in her chosen d-dimensional space encoded in terms of Minkowski modes. An accelerating observer (Bob or Eve depending on the scenario) intercepts this, but using an apparatus that detects excitations of the quantum field defined according to the prescription of the Rindler quantum field theory. So the state that she detects will be described by some infinite-dimensional density matrix. A detailed analysis of this density matrix makes it possible to extract quantitative information about the private and quantum capacities. We evaluate both the quantum capacity from Alice to an accelerating Bob *and* the private capacity for inertial Alice and Bob trying to exchange quantum information while simultaneously confounding an accelerating eavesdropper. Figure 1 contains spacetime diagrams illustrating the two communication scenarios.

Both quantities exhibit surprising behavior. The quantum capacity, the optimal rate at which a sender can transmit qubits to a receiver through some noisy channel, usually exhibits a threshold behavior; channels below some quality threshold have quantum capacity exactly zero. For the Unruh channels, however, we find that the quantum capacity is strictly positive for all accelerations, reaching zero only in the limit of infinite acceleration. It is therefore always possible to transmit quantum data to an accelerating receiver provided the sender is not behind the receiver's horizon. Careful choices of encoding

can therefore eliminate the degradation in fidelity known to occur if one uses a naive teleportation protocol to communicate with an accelerating receiver [3] (see also [42]). In addition to characterizing quantum transmission to an accelerating receiver, our analysis applies equally well to the study of quantum data transmission through an optical amplifier, which may well be its more important application.

The private quantum capacity is likewise positive for all nonzero eavesdropper accelerations. Thus, in principle, any eavesdropper acceleration, no matter how small, can be exploited to safeguard transmissions of quantum data between two inertial observers. Curiously, the private quantum capacity has a simple formula when the channel between the inertial observers is noiseless; the formula reveals that in this case the private quantum capacity is exactly equal to the entanglement-assisted quantum capacity to the eavesdropper's environment, despite the absence of any entanglement assistance in the problem.

1.1 Structure of the paper

Section 2.1 reviews the definition of the quantum capacity and states the Lloyd-Shor-Devetak theorem, which provides the best known achievable rates for quantum data transmission over noisy channels. Section 2.2 introduces the private quantum capacity and proves a capacity theorem in the case where the channel to the intended recipient is noiseless. Section 3.1 reviews the Unruh effect, which then allows for an analysis of the output density matrix of the Unruh channel in Section 3.2. Section 4 is devoted to the explicit capacity calculations.

1.2 Notation

If A and B are two Hilbert spaces, we write $AB \equiv A \otimes B$ for their tensor product. The Hilbert spaces on which linear operators act will be denoted by a subscript. For instance, we write φ_{AB} for a density operator on AB. Partial traces will be abbreviated by omitting subscripts, such as $\varphi_A \equiv \mathrm{Tr}_B \varphi_{AB}$. We use a similar notation for pure states, e.g. $|\psi\rangle_{AB} \in AB$, while abbreviating $\psi_{AB} \equiv |\psi\rangle\langle\psi|_{AB}$. We will write id_A for the identity channel acting on A. In general, the phrase *quantum channel* refers to a completely positive, trace-preserving linear map. The symbol $\mathbb{I}_A$ will be reserved for the identity matrix acting on the Hilbert space A and $\pi_A = \mathbb{I}_A / \dim A$ for the maximally mixed state on A. The identity with a superscript $\mathbb{I}^{(k)}$ used in Sec. 3.2 and onwards acts on a $\binom{d+k-1}{k}$-dimensional Hilbert space. The symbol Φ will be reserved for maximally entangled states and, in particular, $|\Phi_{2^k}\rangle = 2^{-k/2} \sum_{j=1}^{2^k} |j\rangle |j\rangle$ will denote the maximally entangled state on k pairs of qubits.

The trace norm of an operator, $\|X\|_1$ is defined to be $\mathrm{Tr}\,|X| = \mathrm{Tr}\,\sqrt{X^\dagger X}$. The similarity of two density operators φ and ψ can be measured by *trace distance* $\frac{1}{2}\|\varphi - \psi\|_1$, which is equal to the maximum over all possible measurements of the variational distance between the outcome probabilities for the two states. The trace distance is zero

for identical states and one for perfectly distinguishable states.

A complementary measure is the mixed state fidelity

$$F(\varphi, \psi) = \left\| \sqrt{\varphi}\sqrt{\psi} \right\|_1^2 = \left(\operatorname{Tr} \sqrt{\sqrt{\varphi}\psi\sqrt{\varphi}} \right)^2, \tag{1}$$

defined such that when one of the states is pure, $F(\varphi, \psi) = \operatorname{Tr} \varphi\psi$. More generally, the fidelity is equal to one for identical states and zero for perfectly distinguishable states.

For a density operator σ_{AB}, let $H(A)_\sigma$ be the von Neumann entropy of σ_A. The *mutual information* $I(A;B)_\sigma$ is $H(A)_\sigma + H(B)_\sigma - H(AB)_\sigma$ while the *coherent information* is $I(A\rangle B)_\sigma = H(B)_\sigma - H(AB)_\sigma$. The latter quantity, as the negation of the concave conditional entropy $H(A|B)_\sigma = H(AB)_\sigma - H(B)_\sigma$, can be positive only when the state σ is entangled.

For more information on the properties of quantum channels or the functions defined here, we refer the reader to Nielsen and Chuang [39].

2 Standard and Private Quantum Capacities

The objective of the paper will be to evaluate two quantities characterizing communication over the qudit Unruh channels: their quantum capacity and private quantum capacity. While the quantum capacity of a quantum channel has been studied in great detail [5, 36, 43, 20, 28, 29, 31, 34], the private quantum capacity of a wiretap channel has not. A recent paper by Brandão and Oppenheim does, however, consider the very interesting and somewhat related problem of using a fixed, shared quantum state supplemented by public communication to securely transmit quantum information [10]. After briefly introducing the quantum capacity we will therefore develop the general theory of the private quantum capacity, rigorously demonstrating results that were only briefly sketched in [9].

2.1 Quantum Capacity

The ability of a quantum channel to transmit quantum information is measured by its quantum capacity, the optimal rate at which qubits can be reliably transmitted in the limit of many uses of the channel and vanishing error. There are many equivalent ways to define the quantum capacity [35]. Here we use a version which focuses on the transmission of halves of maximally entangled states across the noisy channel. Recall that $\left|\Phi_{2^k}\right\rangle$ represents the maximally entangled state on k pairs of qubits.

Definition 1. An (n, k, δ) *entanglement transmission code* from Alice to Bob consists of an encoding channel $\mathcal{A}$ taking a k-qubit system R' into the input of $\mathcal{N}^{\otimes n}$ and a decoding channel $\mathcal{B}$ taking the output of $\mathcal{N}^{\otimes n}$ to a k-qubit system $C \cong R'$ satisfying

$$\left\| (\mathrm{id} \otimes \mathcal{B} \circ \mathcal{N}^{\otimes n} \circ \mathcal{A})(\Phi_{2^k}) - \Phi_{2^k} \right\|_1 \leq \delta. \tag{2}$$

A rate Q is an *achievable rate* for entanglement transmission if for all $\delta > 0$ and sufficiently large n there exist $(n, \lfloor nQ \rfloor, \delta)$ entanglement transmission codes. The *quantum capacity* $Q(\mathcal{N})$ is the supremum of all the achievable rates.

In any capacity problem, the objective is to understand the structure of the optimal codes. Doing so normally results in a theorem characterizing the capacity in terms of simple entropic functions optimized over a single use of the channel, a so-called "single-letter formula." In general, the structure of the optimal codes is still unknown for the quantum capacity problem. We will see below, however, that they can be characterized in the case of qudit Unruh channels.

The following theorem gives the best known general achievable rates for the quantum capacity problem in terms of the coherent information, as defined in the previous section.

Theorem 2 (Lloyd-Shor-Devetak [36, 43, 20])**.** Let $\left|\psi\right\rangle_{A'A}$ be a pure state, $\mathcal{N}$ a quantum channel from A to B and define $\rho = (\mathrm{id}_{A'} \otimes \mathcal{N})(\psi)$. The quantum capacity $Q(\mathcal{N})$ of $\mathcal{N}$ is at least $I(A'\rangle B)_\rho$.

Note that while $I(A'\rangle B)_\rho$ is expressed as a function of the pure state $\left|\psi\right\rangle^{A'A}$, it is left invariant by unitary transformations of the A' system and can, therefore, equally well be written as a function of the reduced density operator ψ^A. We will make use of that invariance in our calculations.

2.2 Private Quantum Capacity: General Case

The private quantum capacity is the optimal rate at which a sender (Alice) can send qubits to a receiver (Bob) while simultaneously ensuring that those qubits remain encrypted from the eavesdropper's (Eve's) point of view. At first glance, this would not seem to be a very interesting concept. The impossibility of measuring quantum information without disturbing it would seem to ensure that successful transmission of quantum information would make it automatically private. One can imagine a passive eavesdropper, however, who *could* have nontrivial access to the qubits should she choose to exercise it. The setting we will ultimately be primarily concerned with here is a relativistic version of that passive eavesdropper, in particular, the case in which the eavesdropper is uniformly accelerated.

Definition 3. A **quantum wiretap channel** consists of a pair of quantum channels $(\mathcal{N}_{A\to B}, \mathcal{E}_{A\to E})$ taking the density operators on A to those on B and E, respectively.

$\mathcal{N}$ should be interpreted as the channel from Alice to Bob and $\mathcal{E}$ the channel from Alice to Eve. Let $U_\mathcal{N} : A \to B \otimes B_c$ and $U_\mathcal{E} : A \to E \otimes E_c$ be isometric extensions of the channels $\mathcal{N}$ and $\mathcal{E}$. In particular, $\mathcal{N}(\cdot) = \mathrm{Tr}_{B_c} U_\mathcal{N} \cdot U_\mathcal{N}^\dagger$ and $\mathcal{E}(\cdot) = \mathrm{Tr}_{E_c} U_\mathcal{E} \cdot U_\mathcal{E}^\dagger$. In many circumstances, $\mathcal{E}$ will be a degraded version of the "environment" of the Alice-Bob channel, meaning that there exists a channel $\mathcal{D}$ such that $\mathcal{E}(\cdot) = \mathcal{D} \circ \mathrm{Tr}_B U_\mathcal{N} \cdot U_\mathcal{N}^\dagger$. For the uniformly accelerated eavesdropper, however, this needn't be the case so we

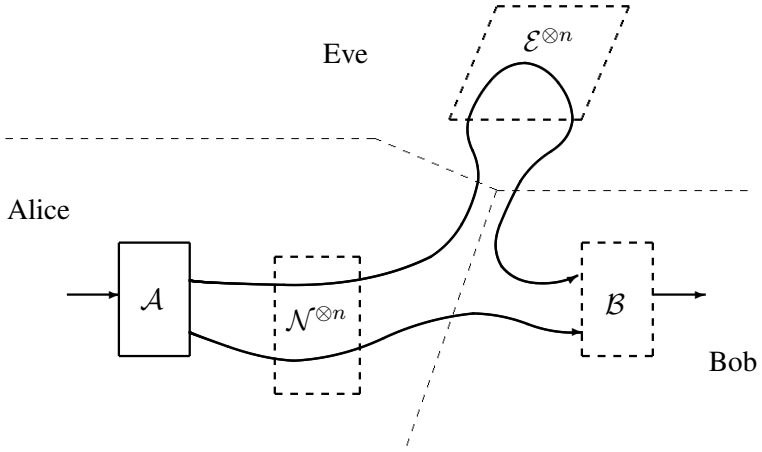

Figure 2: Another scenario in which the wiretap framework applies. Alice sends quantum data to Bob through two separate channels, two different fiber optic links, for example. Eve potentially has access to one of the links and Alice wants to ensure that should Eve try to eavesdrop that she will not learn anything about the transmission. The map $\mathcal{N}^{\otimes n}$ would represent all the noise experienced by both transmission lines while Eve's channel $\mathcal{E}^{\otimes n}$ would describe the output of the transmission line entering her domain, not including any further noise it experiences before finally ending in Bob's laboratory. The dotted lines indicate that $\mathcal{N}^{\otimes n}$ and $\mathcal{E}^{\otimes n}$ should not be composed; each is a complete description of the noise experienced by Bob and Eve, respectively.

don't require *a priori* that there be a particular relationship between $\mathcal{N}$ and $\mathcal{E}$. Another relevant example is illustrated in Figure 2.

Recall that $\pi_{2^k} = \mathbb{I}/2^k$, the maximally mixed state on k qubits.

Definition 4. An (n, k, δ, ϵ) **private entanglement transmission code** from Alice to Bob consists of an encoding channel $\mathcal{A}$ taking a k-qubit system R' into the input of $\mathcal{N}^{\otimes n}$ and a decoding channel $\mathcal{B}$ taking the output of $\mathcal{N}^{\otimes n}$ to a k-qubit system $C \cong R'$ satisfying

1. Transmission: $\|(\mathrm{id} \otimes \mathcal{B} \circ \mathcal{N}^{\otimes n} \circ \mathcal{A})(\Phi_{2^k}) - \Phi_{2^k}\|_1 \leq \delta$.
2. Privacy: $\|(\mathrm{id} \otimes \mathcal{E}^{\otimes n} \circ \mathcal{A})(\Phi_{2^k}) - \pi_{2^k} \otimes (\mathcal{E}^{\otimes n} \circ \mathcal{A})(\pi_{2^k})\|_1 \leq \epsilon$.

A rate Q is an **achievable rate** for private entanglement transmission if for all $\delta, \epsilon > 0$ and sufficiently large n there exist $(n, \lfloor nQ \rfloor, \delta, \epsilon)$ private entanglement transmission codes. The **private quantum capacity** $Q_p(\mathcal{N}, \mathcal{E})$ is the supremum of all the achievable rates.

The transmission criterion states that halves of EPR pairs encoded by $\mathcal{A}$, sent through the channel and then decoded by $\mathcal{B}$ will be preserved by the communications system

with high fidelity. Alternatively, one could ask that arbitrary pure states or even arbitrary states entangled with a reference sent through $\mathcal{B} \circ \mathcal{N}^{\otimes n} \circ \mathcal{A}$ be preserved with high fidelity. The different definitions are equivalent for the standard quantum capacity $Q(\mathcal{N}) = Q_p(\mathcal{N}, \mathrm{Tr})$, which is defined with no privacy requirement [35]. The equivalence extends straightforwardly to the private quantum capacity.

The privacy condition can also be written in a slightly more indirect but illustrative way. If $\Psi_{RE^n} = (\mathrm{id}_R \otimes \mathcal{E}^{\otimes n} \circ \mathcal{A})(\Phi_{2^k})$, then the condition states that

$$\|\Psi_{RE^n} - \Psi_R \otimes \Psi_{E^n}\|_1 \leq \epsilon. \tag{3}$$

In words, the channel $\mathcal{E}^{\otimes n} \circ \mathcal{A}$ should destroy all correlations with R for the input maximally entangled state Φ_{2^k}.

Let $\mathcal{E}_c(\cdot) = \mathrm{Tr}_E U_{\mathcal{E}} \cdot U_{\mathcal{E}}^\dagger$ be the channel from Alice to the environment of the channel to Eve. The output of $\mathcal{E}_c$ contains data that Eve is incapable of intercepting, which explains its appearance in our main capacity theorem:

Theorem 5 (Private quantum capacity)**.** The private quantum capacity $Q_p(\mathrm{id}, \mathcal{E})$ when the channel from Alice to Bob is noiseless is given by the formula $\max \frac{1}{2} I(A'; E_c)_\rho$, where the maximization is over all pure states $|\psi\rangle_{A'A}$ and $\rho = (\mathrm{id} \otimes \mathcal{E}_c)(\psi)$.

Because the mutual information is equal to zero only for product states, $Q_p(\mathrm{id}, \mathcal{E})$ is zero only when $\mathcal{E}_c$ is the constant channel or, equivalently, $\mathcal{E}$ is the identity. In particular, it is not necessary for $\mathcal{E}_c$ to have nonzero quantum capacity in order for $Q_p(\mathrm{id}, \mathcal{E})$ to be positive. The fact that the optimization is over input states to a single copy of $\mathcal{E}$ is notable: the number of such "single-letter" results in quantum Shannon theory is very limited. No single-letter formulas are known for the classical or quantum capacities of general quantum channels, for example.

Despite the absence here of any entanglement assistance, the theorem implies that $Q_p(\mathrm{id}, \mathcal{E})$ is exactly equal to the entanglement-assisted quantum capacity of $\mathcal{E}_c$, usually written $Q_E(\mathcal{E}_c)$, by virtue of the fact that their formulas match [6]. Why they should be the same is, however, something of a mystery.

We will break the proof of Theorem 5 into two parts, the achievability of the claimed rate and then a converse showing that it is impossible to do better. The strategy is illustrated in Figure 3.

The achievability part relies on the following simple lemma:

Lemma 6. Let $|\rho\rangle_{AB}$ be a bipartite pure state and $|\psi\rangle_A$ a pure state of A. If $\|\rho_A - \psi_A\|_1 \leq \kappa$ then there exists a pure state $|\omega\rangle_B$ such that $\|\rho_{AB} - \psi_A \otimes \omega_B\|_1 \leq 2\sqrt{\kappa}$.

Proof. Recall that, for all states ϕ and τ, the mixed state fidelity function satisfies

$$F(\phi, \tau) \geq 1 - \|\phi - \tau\|_1 \tag{4}$$

$$\text{and} \quad \|\phi - \tau\|_1 \leq 2\sqrt{1 - F(\phi, \tau)}. \tag{5}$$

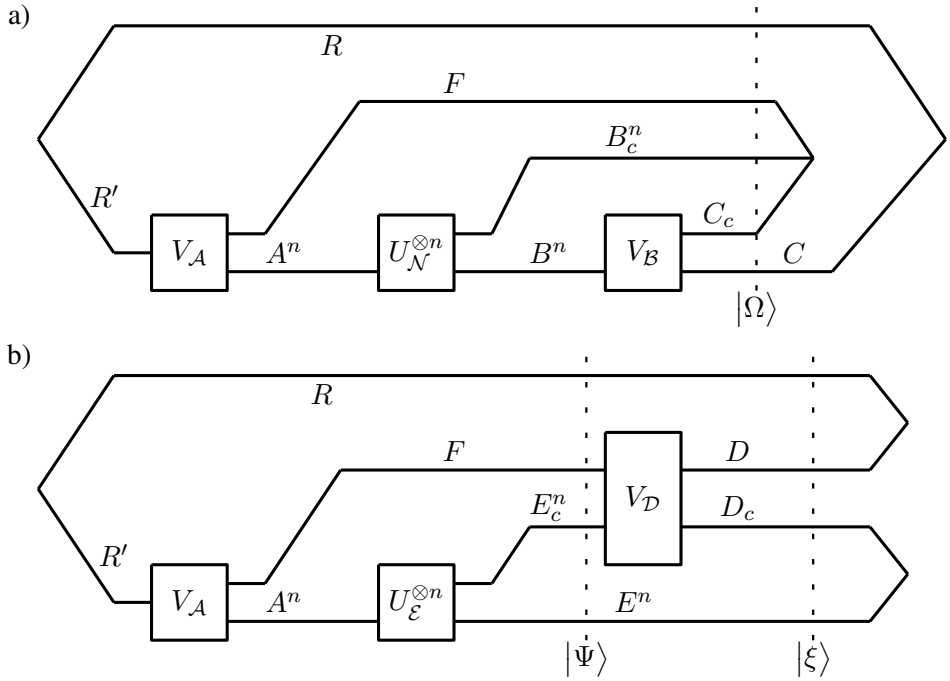

Figure 3: Structure of a quantum privacy code. $V_{\mathcal{A}}$, $U_{\mathcal{N}}$, $U_{\mathcal{E}}$, $V_{\mathcal{B}}$ and $V_{\mathcal{D}}$ are isometric extensions of $\mathcal{A}$, $\mathcal{N}$, $\mathcal{E}$, $\mathcal{B}$ and $\mathcal{D}$, respectively. The initial state is maximally entangled between R and R' and, because all the transformations are isometries, the state remains pure as time increases from left to right. Registers meeting at a vertex on the right hand side of the diagram are generically correlated while those not meeting will be product. (a) The transmission condition states that using only the output of $\mathcal{N}^{\otimes n}$, Bob should be able to produce the purification of the reference entanglement. This implies, in particular, that the reduced state on $R \otimes F$ is nearly product, a fact used in the converse proof. (b) The privacy condition requires that the state on $R \otimes E^n$ be nearly product. That is equivalent to the existence of a decoding channel $\mathcal{D}$ (with isometric extension $V_{\mathcal{D}}$) acting on $E_c^n \otimes F$ whose output approximates a purification of the reference entanglement R. The code construction demonstrates the existence of such a $\mathcal{D}$. Note that while both $\mathcal{B}$ and $\mathcal{D}$ decode the same quantum information, they cannot be applied simultaneously so the no-cloning theorem is not violated.

(See, for example, [39].) So, by the hypothesis of the lemma, $F(\rho_A, \psi_A) \geq 1 - \kappa$. But by Uhlmann's theorem [44, 32],

$$F(\rho_A, \psi_A) = \max_{\left|\omega\right\rangle_B} \left|\left\langle \rho \right|_{AB} \left|\psi\right\rangle_A \left|\omega\right\rangle_B\right|^2 .$$

which completes the proof when combined with (5). ■

We will also need the following variant of the Lloyd-Shor-Devetak theorem:

Theorem 7. Let $\left|\psi\right\rangle_{A'A}$ be a pure state, $\mathcal{N}_j$ a quantum channel from A to B_j for $1 \leq j \leq k$ and $\rho_j = (\mathrm{id}_{A'} \otimes \mathcal{N}_j)(\psi)$. There is a single encoding $\mathcal{A}$ that will achieve entanglement transmission for all j at the rate

$$\min_{1 \leq j \leq k} I(A'\rangle B_j)_{\rho_j}. \tag{6}$$

Proof. This is a special case of Theorem IV.3 of [7] except for the fact that the theorem in question assumes that the output spaces B_j are all identical. To apply the theorem, it therefore suffices to set $B = \oplus_{j=1}^k B_j$ and compose each channel $\mathcal{N}_j$ with the embedding of B_j into B.

Alternatively, one can observe that the encodings used in [28] to achieve entanglement transmission at the coherent information rate depend only on ψ and not on the channels themselves. The analysis therein demonstrates that for sufficiently large n, a random encoding succeeds for a given channel with high probability. Random encodings will therefore succeed for any finite number of channels simultaneously again with high probability. ■

Proof. Achievability part of Theorem 5. Let $V_{\mathcal{A}}$ be an isometric extension of $\mathcal{A}$ with output on $A^n F$. The privacy condition applied to E^n is actually equivalent to entanglement transmission to FE_c^n. To show achievability, it suffices to show that entanglement transmission implies privacy. Indeed, suppose that there exists a "decoding" channel $\mathcal{D}$ from FE_c^n to a space of k qubits on D such that

$$\left\| (\mathrm{id} \otimes \mathcal{D} \circ \mathcal{E}_c^{\otimes n})((\mathbb{I} \otimes V_{\mathcal{A}}) \Phi_{2^k} (\mathbb{I} \otimes V_{\mathcal{A}}^\dagger)) - \Phi_{2^k} \right\|_1 \leq \kappa.$$

Let $V_{\mathcal{D}} : FE_c^n \to DD_c$ be an isometric extension for $\mathcal{D}$. Call $\left|\xi\right\rangle_{RDD_cE^n}$ the purification of $(\mathrm{id} \otimes \mathcal{D} \circ \mathcal{E}_c^{\otimes n})((\mathbb{I} \otimes V_{\mathcal{A}}) \Phi_{2^k} (\mathbb{I} \otimes V_{\mathcal{A}}^\dagger))$. By Lemma 6 and as illustrated in Figure 3b, there exists a pure state $\left|\omega\right\rangle_{D'E^n}$ such that

$$\| \xi_{RDD_cE^n} - (\Phi_{2^k})_{RD} \otimes \omega_{D_cE^n} \|_1 \leq 2\sqrt{\kappa}. \tag{7}$$

By the monotonicity of the trace distance under the partial trace, this implies that

$$\| \xi_{RE^n} - (\pi_{2^k})_R \otimes \omega_{E^n} \|_1 \leq 2\sqrt{\kappa}, \tag{8}$$

which is nothing other than Eq. (3) for $\epsilon = 2\sqrt{\kappa}$.

It is therefore sufficient to find codes that simultaneously perform entanglement transmission to B^n and to FE_c^n, in the first case for the channel $\mathrm{id}_{A^n \to B^n} \otimes \mathrm{Tr}_F$ which traces over F and in the second case for the channel $\mathcal{E}_c^{\otimes n} \otimes \mathrm{id}_F$ whose output combines F with Eve's complementary channel. Applying Theorem 7 to these channels using the input state $\left|\varphi\right\rangle = \left|\psi\right\rangle_{AA'}^{\otimes n} \otimes \left|\Phi\right\rangle_{FF'}$ provides the following pair of conditions sufficient for simultaneous entanglement transmission:

$$\begin{aligned} nQ &< I(A'F'\rangle B^n)_{\psi^{\otimes n} \otimes \Phi_{F'}} && (9)\\ &= H(B^n)_{\psi^{\otimes n}} - H(A'F'B^n)_{\psi^{\otimes n} \otimes \Phi_{F'}} && (10)\\ &= nH(A')_\psi - \log \dim F && (11)\\ \text{and} \quad nQ &< I(A'F'\rangle FE_c^n)_{(\mathrm{id}_{A'F} \otimes \mathcal{E}_c^{\otimes n})(\varphi)} && (12)\\ &= nI(A'\rangle E_c)_\rho + \log \dim F. && (13) \end{aligned}$$

(The expressions use the slight abuse of notation that $\psi_{A'B} = \mathrm{id}_{A \to B}(\psi_{A'A})$.) The simplifications rely only on the facts that the entropy of a product state is the sum of the entropies of the individual factors and that for any pure state $\left|\omega\right\rangle_{XY}$, the nonzero eigenvalues of ω_X and ω_Y are the same so that $H(\omega_X) = H(\omega_Y)$.

Choosing $\dim F = 2^{nf}$ allows us to rewrite these conditions as

$$Q < H(A')_\psi - f \quad \text{and} \quad Q < I(A'\rangle E_c)_\rho + f. \tag{14}$$

The constraints have intuitive interpretations: the first is the noiseless rate to Bob through id_A reduced by the rate at which qubits are lost to F, while the second is the standard coherent information rate for $\mathcal{E}_c$ augmented by a noiseless channel to F. Q is maximized subject to these constraints when $H(A')_\psi - f = I(A'\rangle E_c)_\rho + f$. Using the fact that $H(A)_\psi = H(A')_\rho$ and purifying ρ to $\left|\rho\right\rangle_{A'EE_c}$, this equation can be written as

$$\begin{aligned} f &= \tfrac{1}{2}\left[H(A')_\psi - I(A'\rangle E_c)_\rho\right] && (15)\\ &= \tfrac{1}{2}\left[H(A')_\rho - H(E_c)_\rho + H(A'E_c)_\rho\right] && (16)\\ &= \tfrac{1}{2}\left[H(A')_\rho - H(A'E)_\rho + H(E)_\rho\right] && (17)\\ &= \tfrac{1}{2} I(A';E)_\rho. && (18) \end{aligned}$$

Therefore, the rate Q is achievable provided

$$\begin{aligned} Q &< H(A')_\rho - \tfrac{1}{2} I(A';E)_\rho && (19)\\ &= H(A')_\rho - \tfrac{1}{2}\left[H(A')_\rho - H(A'E)_\rho + H(E)_\rho\right] && (20)\\ &= \tfrac{1}{2}\left[H(A')_\rho + H(E_c)_\rho - H(A'E_c)_\rho\right] && (21)\\ &= \tfrac{1}{2} I(A';E_c)_\rho, && (22) \end{aligned}$$

which is what we set out to prove. ■

It wasn't essential that the channel from Alice to Bob be noiseless until the entropic manipulations in the second half of the proof. Stopping before that point provides the following achievable rates in the general case:

Corollary 8. Let $(\mathcal{N}, \mathcal{E})$ be a quantum wiretap channel. For $|\psi\rangle_{A'A}$ any pure state, $\rho = (\mathrm{id} \otimes \mathcal{N})(\psi)$ and $\tau = (\mathrm{id} \otimes \mathcal{E})(\psi)$, the following lower bound on the private quantum capacity holds:

$$Q_p(\mathcal{N}, \mathcal{E}) \geq \frac{1}{2} \left[I(A'\rangle B)_\rho - I(A'\rangle E)_\tau \right]. \tag{23}$$

The proof of the converse to Theorem 5 will rely on an elegant inequality of Alicki and Fannes [2]:

Lemma 9. Let ρ_{AB} and σ_{AB} be bipartite density operators on finite dimensional systems and let $h_2(x) = -x \log x - (1-x)\log(1-x)$. If $\|\rho_{AB} - \sigma_{AB}\|_1 \leq \varepsilon \leq 1/e$, then

$$|H(A|B)_\rho - H(A|B)_\sigma| \leq 4\epsilon \log \dim A + 2\, h_2(\epsilon). \tag{24}$$

What is notable about the inequality is that the upper bound is independent of the dimension of B. In classical information theory, a similar bound holds but for a trivial reason: if ρ is classical then $H(A|B)_\rho$ is an average of entropies of A alone. No such reduction exists in the quantum case, but $H(A|B)$ nonetheless behaves as if there were in this sense.

We will also need the other half of the equivalence between privacy and entanglement transmission. Specifically, privacy implies entanglement transmission in the following sense:

Lemma 10. Let $V : A \to BB_c$ be an isometric extension of some channel $\mathcal{N}$ from A to B. Fixing a Hilbert space R satisfying $|R| \leq |A|$, let $|\Phi\rangle_{RA}$ be maximally entangled with a subspace of A and set $|\psi\rangle_{RBB_c} = (\mathbb{I}_R \otimes V)|\Phi\rangle_{RA}$. Then there is a "decoding" channel $\mathcal{B}$ from B to $R' \cong R$ satisfying

$$\left\| \Phi_{RR'} - \left(\mathrm{id}_R \otimes \mathcal{B} \circ \mathcal{N} \right)(\Phi_{RA}) \right\|_1 \leq 2 \left\| \psi_{RB_c} - \Phi_R \otimes \psi_{B_c} \right\|_1^{1/2}. \tag{25}$$

Proof. This is a widely used fact in quantum Shannon theory. The proof is similar to that of Lemma 6. For details, see Theorem II of [28], which is an equivalent statement up to an application of Eq. (5).

■

Proof. Converse part of Theorem 5. To prove optimality, suppose we have an $(n, \lfloor nQ \rfloor, \delta, \epsilon)$ private entanglement transmission code. As before, use R to denote the reference space for the maximally entangled state Φ_{2^k} in the definition, with $k = \lfloor nQ \rfloor$. Let $|\Psi\rangle_{RFE^n E_c^n}$ be the purified final state after $\mathcal{E}^{\otimes n} \circ \mathcal{A}$ has acted on Φ_{2^k}. The privacy condition $\|\Psi_{RE^n} - \Psi_R \otimes \Psi_{E^n}\|_1 \leq \epsilon$ and Lemma 10 imply that there exists a "decoding" channel $\mathcal{D}$ on $E_c^n F$ such that

$$\left\| \Phi_{2^k} - (\mathrm{id}_R \otimes \mathcal{D})(\Psi_{RFE_c^n}) \right\|_1 \leq 2\sqrt{\epsilon}. \tag{26}$$

The Alicki-Fannes inequality (Lemma 9) then implies that there is a function $g_1(\epsilon)$ satisfying $\lim_{\epsilon\to 0} g_1(\epsilon) = 0$ such that

$$2\lfloor nQ \rfloor = I(R;A)_{\Phi_{2^k}} \leq I(R;A)_{(\mathrm{id}_R \otimes \mathcal{D})(\Psi)} + ng_1(\epsilon). \tag{27}$$

The monotonicity of the mutual information under quantum channels then implies that

$$\begin{aligned} I(R;A)_{(\mathrm{id}_R \otimes \mathcal{D})(\Psi)} &\leq I(R;E_c^n F)_\Psi & (28)\\ &= I(R;F)_\Psi + I(R;E_c^n|F)_\Psi, & (29)\end{aligned}$$

where the second line is just the chain rule for mutual information. Now consider $I(R;F)_\Psi$. The entanglement transmission condition requires that

$$\left\| (\mathrm{id} \otimes \mathcal{B} \circ \mathcal{N}^{\otimes n} \circ \mathcal{A})(\Phi_{2^k}) - \Phi_{2^k} \right\|_1 \leq \delta \tag{30}$$

Let $\left|\Omega\right\rangle_{RFB_c^n CC_c}$ be a purification of $(\mathrm{id}_R \circ \mathcal{B} \circ \mathcal{N}^{\otimes n} \circ A)(\Phi_{2^k})$, where B_c is the environment of $\mathcal{N}^{\otimes n}$ and C_c the environment of $\mathcal{B}$. The entanglement transmission condition and Lemma 6 together imply that there is a state $\xi_{FB_c{}^n C_c}$ such that

$$\begin{aligned} 2\sqrt{\delta} &\geq \left\| \Omega_{RFB_c{}^n CC_c} - (\Phi_{2^k})_{RC} \otimes \xi_{FB_c{}^n C_c} \right\|_1 & (31)\\ &\geq \left\| \Omega_{RF} - \pi_R \otimes \xi_F \right\|_1, & (32)\end{aligned}$$

where the second inequality is a consequence of the monotonicity of the trace distance under the partial trace. But $\Psi_{RF} = \Omega_{RF}$ since neither $\mathcal{E}^{\otimes n}$ nor $\mathcal{B} \circ \mathcal{N}^{\otimes n}$ acts on RF. So, again by the Alicki-Fannes inequality, there is a function $g_2(\delta)$ satisfying $\lim_{\delta\to 0} g_2(\delta) = 0$ such that

$$I(R;F)_\Psi \leq ng_2(\delta). \tag{33}$$

Combining Eqs. (27), (29) and (33) then gives

$$2\lfloor nQ \rfloor \leq I(R;E_c^n|F)_\Psi + n[g_1(\epsilon) + g_2(\delta)]. \tag{34}$$

But

$$I(R;E_c^n|F)_\Psi = I(RF;E_c^n)_\Psi - I(E_c^n;F)_\Psi \leq I(RF;E_c^n)_\Psi \tag{35}$$

by the chain rule and the nonnegativity of mutual information. Thus, we finally arrive at the conclusion that

$$2\lfloor nQ \rfloor \leq I(RF;E_c^n)_\Psi + n[g_1(\epsilon) + g_2(\delta)]. \tag{36}$$

The composite system RF can be thought of as the purification of the input to the channel, which is the role played by A' in Theorem 5. Relabeling RF by A' and recalling that the inequality must hold for all $\delta, \epsilon > 0$ and n sufficiently large then shows that

$$Q_p(\mathrm{id}, \mathcal{E}) \leq \lim_{n\to\infty} \max \frac{1}{2n} I(A';E_c^n)_\rho, \tag{37}$$

where the maximization is over pure states $\left|\psi\right\rangle_{A'^n A^n}$ and $\rho = (\mathrm{id} \otimes \mathcal{E}_c^{\otimes n})(\psi)$. It is well-known, however, that fixing $n = 1$ does not affect the expression on the right hand side of the inequality, which is the entanglement-assisted quantum capacity of $\mathcal{E}_c$ [6]. That completes the proof of the converse. ■

3 The qudit Unruh channel: Definition and structure

In this section we define the qudit Unruh channel and determine the structure of the output density matrix. One of the key consequences of the structure theorem will be the covariance of the qudit Unruh channel with respect to the $SU(d)$ group.

3.1 The Unruh effect

In order to describe the Unruh effect it will be useful to briefly recapitulate the construction of a quantum field theory. One begins with the classical field theory and its space of solutions. One uses the "time" coordinate to define a space of positive-frequency solutions, this is taken as the Hilbert space of "one-particle" states, $\mathcal{H}$. One then constructs the usual Fock space, $\mathcal{F}(\mathcal{H})$ over this Hilbert space. This Fock space comes with its usual apparatus of annihilation and creation operators, $a_k, a_k^\dagger$ respectively. The vacuum state is the unique state killed by all the a_k.

In Minkowski space one has the usual quantization procedure based on the usual timelike Killing field that yields a Hilbert space $\mathcal{H}_M$ with a Fock space $\mathcal{F}(\mathcal{H}_M)$ and a vacuum state that we call $\left|vac\right\rangle_M$. We can, however, use another timelike Killing field ξ, the one whose integral curves are the trajectories of an accelerating observer. For such an observer the spacetime consists of 4 regions as shown in Figure 4. If we look at positive frequency states with respect to this notion of time, we can divide them into solutions that live in the left wedge and those that live in the right wedge. We get two Hilbert spaces, $\mathcal{H}_L, \mathcal{H}_R$ and their respective Fock spaces $\mathcal{F}(\mathcal{H}_L), \mathcal{F}(\mathcal{H}_R)$. The space of one-particle states appropriate to the accelerating observer, we shall call her the Rindler observer, is $\mathcal{H}_{Rin} \simeq \mathcal{H}_L \oplus \mathcal{H}_R$ We have that $\mathcal{F}(\mathcal{H}_{Rin}) \simeq \mathcal{F}(\mathcal{H}_L) \otimes \mathcal{F}(\mathcal{H}_R)$. The transformation from the Minkowski observer's Fock space to the Rindler observer's Fock space is given by a map $S : \mathcal{F}(\mathcal{H}_M) \to \mathcal{F}(\mathcal{H}_{Rin})$. The Minkowski vacuum $\left|vac\right\rangle_M$ will appear as $S\left|vac\right\rangle_M$ in the quantum field theory of the Rindler spacetime The accelerating observer can only perceive states of $\mathcal{F}(\mathcal{H}_R)$ so the correct description of how she perceives the state is obtained by tracing out the states of $\mathcal{F}(\mathcal{H}_L)$. Thus, she sees a mixed state. The transformation S takes the vacuum state $\left|vac\right\rangle_M$ to an infinite product state corresponding to all possible modes, and in fact the Minkowski and Rindler field theories are not unitarily equivalent [47]. (This may appear to contradict the statement above that there is a map S between the Fock spaces. The point is that there is no such *unitary* S between the indicated Fock spaces.)

In this paper we will use a fixed number of input modes and restrict attention to a fixed number of modes of the output rather than all possible modes. Physically we can think of the Rindler observer's detector being tuned to some *finite number of modes*. The Fock space that we get this way is unitarily equivalent to the input Fock space also restricted to these modes, so we can define a unitary transformation between the input and output spaces, where the output is the restricted Fock space for both Rindler wedges. We now proceed with the mathematical details.

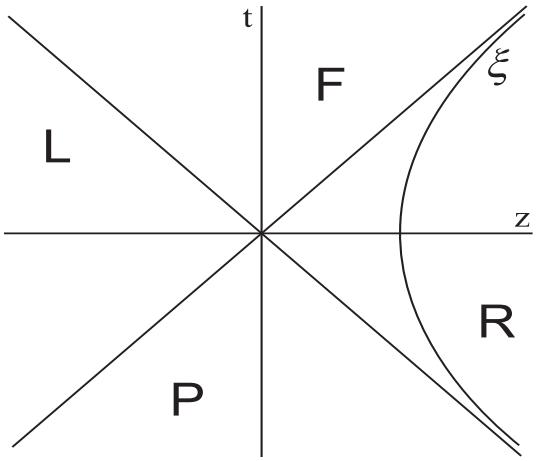

Figure 4: Illustration of a timelike Killing field ξ chosen for a uniformly accelerating observer. The letters F, R, P and L stand for future, right, past and left cone, respectively.

The solution of the Klein-Gordon equation for a real massless scalar field in Minkowski spacetime can be expanded in terms of the so-called Unruh modes $U_{\pm\Omega,\mathbf{k}}$ [16]

$$\phi_{Unr} = \int_0^\infty d\Omega \int_{-\infty}^\infty d\mathbf{k} \left[d_{\Omega,\mathbf{k}} U_{\Omega,\mathbf{k}} + d^\dagger_{\Omega,\mathbf{k}} \bar{U}_{\Omega,\mathbf{k}} + d_{-\Omega,\mathbf{k}} U_{-\Omega,\mathbf{k}} + d^\dagger_{-\Omega,\mathbf{k}} \bar{U}_{-\Omega,\mathbf{k}} \right]. \tag{38}$$

The bar denotes complex conjugation and the field coefficients $d_{\pm\Omega,\mathbf{k}}, d^\dagger_{\pm\Omega,\mathbf{k}}$ are the (Unruh) bosonic creation and annihilation operators satisfying $\left[d_{\pm\Omega,\mathbf{k}}, d^\dagger_{\pm\Omega',\mathbf{k}'}\right] = \delta(\mathbf{k}-\mathbf{k}')\delta(\Omega-\Omega')$ with any other combination equal to zero. Similarly, if we introduce the spacetime of a uniformly accelerating observer (Rindler spacetime) the same field can be expanded in terms of the left and right Rindler modes $R^\pm_{\Omega,\mathbf{k}}$

$$\phi_{Rin} = \int_0^\infty d\Omega \int_{-\infty}^\infty d\,\mathbf{k} \left[b^R_{\Omega,\mathbf{k}} R^+_{\Omega,\mathbf{k}} + b^{R^\dagger}_{\Omega,\mathbf{k}} \bar{R}^+_{\Omega,\mathbf{k}} + b^L_{\Omega,\mathbf{k}} R^-_{\Omega,\mathbf{k}} + b^{L^\dagger}_{\Omega,\mathbf{k}} \bar{R}^-_{\Omega,\mathbf{k}} \right]. \tag{39}$$

The number Ω is the mode frequency divided by Rindler observer's proper acceleration and $\mathbf{k}$ is the mode three-momentum.

The relation between the different modes is as follows [45, 16]. One can define Minkowski modes using plane waves according to the standard Minkowski coordinates. The Unruh modes of Eq. (38) are linear combinations of Minkowski modes. They are, however, parametrized by the quantities Ω and $\mathbf{k}$ that refer to the accelerated observer. The annihilation operators associated with the Unruh modes are linear combinations of annihilation operators of the Minkowski modes, i.e. they are not mixed with the Minkowski creation operators and they also annihilate the Minkowski vacuum. They serve as a convenient intermediate set of modes in going from the Minkowski field theory to the Rindler field theory. The Rindler modes are the ones defined using the positive and negative frequency decomposition of the accelerating observer. When related

to the Minkowski modes they will have a mixture of positive and negative frequency Minkowski modes. The equations above give the expansion of the *same* field operator in terms of the two different modes.

The Rindler annihilation and creation operators come in two pairs associated with the left and right wedges; the ones associated with the right wedge are denoted by $b^R_{\Omega,\mathbf{k}}$ and $b^{R^\dagger}_{\Omega,\mathbf{k}}$. They separately satisfy the same commutation relations as the Unruh operators. Comparing both expressions for what are in fact the same the field operators we get the Bogoliubov transformation between the Unruh and Rindler creation and annihilation operators

$$\begin{pmatrix} b^R_{\Omega,\mathbf{k}} \\ b^{L^\dagger}_{\Omega,-\mathbf{k}} \end{pmatrix} = \begin{pmatrix} \cosh r & \sinh r \\ \sinh r & \cosh r \end{pmatrix} \begin{pmatrix} d_{-\Omega,\mathbf{k}} \\ d^\dagger_{\Omega,-\mathbf{k}} \end{pmatrix}, \tag{40}$$

where $\cosh r = \sqrt{e^\Omega/(e^\Omega-1)}, \sinh r = \sqrt{1/(e^\Omega-1)}$ [16, 47]. We use the natural units $\hbar = c = 1$. The transformation completely describes the physics of a uniformly accelerated observer. We are able to calculate the expectation values of any Rindler operator in terms of the Unruh modes. The celebrated thermal spectrum of the Minkowski vacuum as seen by the Rindler observer is an example of such a calculation. In Eq. (40) we witness another advantage of working with Unruh modes: the transformation between Unruh and Rindler modes is very simple.

Inverting Eq. (40) we can see that every Unruh Fock state can be expanded as a function of the left and right Rindler modes. In other words, there is an operation $\mathcal{O}$ assigning a two-mode entangled Rindler state to every state from Minkowski spacetime:

$$\mathcal{O} : \left|n\right\rangle_{Unr} \mapsto \prod_{\Omega,\mathbf{k}} \frac{1}{\cosh^{1+n} r} \sum_{m=0}^{\infty} \binom{n+m}{n}^{1/2} \tanh^m r \left|(n+m)^L_{\Omega,-\mathbf{k}}\right\rangle_{Rin} \left|m^R_{\Omega,\mathbf{k}}\right\rangle_{Rin}. \tag{41}$$

The mathematical reason that the transformation between the two Fock representations is not unitary [47] is the presence of the infinite product. An obvious way to circumvent this problem is to restrict to just one output mode of the operation $\mathcal{O}$. We would like to find a unitary operation "emulating" the action of the restricted $\mathcal{O}$. Effectively, it is the same as introducing a two-mode unitary transformation

$$U_{AC}(r) = \exp\left[r(a^\dagger c^\dagger - ac)\right]. \tag{42}$$

This formulation deliberately uses a different mode notation (the labels $A \equiv (\Omega, \mathbf{k})$ and $C \equiv (\Omega, -\mathbf{k})$), the reason being that the output mode restriction allows us to work in a single Hilbert space. We stress that the unitary transformation Eq. (42) produces the "correct" states Eq. (41) as seen by a Rindler observer. The shortened notation also avoids carrying too many indices with all the mode information. The two different symbols A and C correspond to the operators a and c, respectively. Therefore $U_{AC}(r)$ acts as

$$U_{AC}(r) \left|n\right\rangle_A \left|vac\right\rangle_C = \frac{1}{\cosh^{1+n} r} \sum_{m=0}^{\infty} \binom{n+m}{n}^{1/2} \tanh^m r \left|n+m\right\rangle_A \left|m\right\rangle_C. \tag{43}$$

Now suppose we want to transform an arbitrary (pure) qudit. There are many ways to encode a logical qudit, but we will restrict to a natural method known as multi-rail encoding, in which an arbitrary qudit state takes the form

$$\left|\psi\right\rangle_A = \sum_{i=1}^{d} \beta_i a_i^\dagger \left|vac\right\rangle_A . \tag{44}$$

In other words, there are d distinguishable modes and the unitary acts on each mode to give

$$\left|\sigma\right\rangle_{AC} = \bigotimes_{i=1}^{d} U_{A_iC_i} \left|\psi\right\rangle_{AC}, \tag{45}$$

where $\left|\psi\right\rangle_{AC} = \left|\psi\right\rangle_A \left|vac\right\rangle_C$. The disentangling theorem allows us to rewrite the exponential as [4]

$$\begin{aligned} U_{A_iC_i}(r) = \frac{1}{\cosh r} \exp\left[\tanh r\, a_i^\dagger c_i^\dagger\right] \\ \times \exp\left[-\ln\cosh r (a_i^\dagger a_i + c_i^\dagger c_i)\right] \exp\left[-\tanh r\, a_i c_i\right]. \end{aligned} \tag{46}$$

Using the commutation relations $[a_i^\dagger, a_j^\dagger] = [a_i, c_j^\dagger] = [a_i, c_j] = 0$, the action of U_{AC} simplifies to

$$U_{AC}\left|\psi\right\rangle_{AC} = \bigotimes_{i=1}^{d} U_{A_iC_i}\left|\psi\right\rangle_{AC} = \frac{1}{\cosh^{d+1} r} \exp\left[\tanh r \left(\sum_{i=1}^{d} a_i^\dagger c_i^\dagger\right)\right] \left|\psi\right\rangle_{AC} . \tag{47}$$

Note that this simplification holds only when U transforms states from the Hilbert space spanned by the multi-rail basis. The summands in the Taylor series for U can be simplified by the multinomial theorem to give

$$\frac{\tanh^k r}{k!}\left(\sum_{i=1}^{d} a_i^\dagger c_i^\dagger\right)^k = \tanh^k r \sum_{l_1+\ldots+l_d=k} \frac{1}{l_1!\ldots l_d!} (a_1^\dagger c_1^\dagger)^{l_1} \ldots (a_d^\dagger c_d^\dagger)^{l_d}. \tag{48}$$

The simplified expression Eq. (47) allows us to rewrite Eq. (45) in the following way:

$$\begin{aligned} \left|\sigma\right\rangle_{AC} &= \left(\sum_{i=1}^{d} \beta_i a_i^\dagger\right) U \left|vac\right\rangle \\ &= \frac{1}{\cosh^{d+1} r}\left(\sum_{i=1}^{d} \beta_i a_i^\dagger\right) \sum_{k=0}^{\infty} \tanh^k r \sum_{l_1+\ldots+l_d=k} \left|l_1\ldots l_d\right\rangle_A \left|l_1\ldots l_d\right\rangle_C, \end{aligned} \tag{49}$$

where $1/\sqrt{l_i!}(a_i^\dagger)^{l_i}\left|vac\right\rangle = \left|l_i\right\rangle$ has been used in the second line. Thus, an input state $\left|\psi\right\rangle_A$ of the from Eq. (44) gets transformed to a final output state

$$\left|\sigma\right\rangle_{AC} = \frac{1}{\cosh^{d+1} r} \sum_{k=1}^{\infty} \tanh^{k-1} r \sum_{I} \left[\sum_{i=1}^{d} \beta_i \sqrt{l_{I,i}+1}\left|I^{(i)}\right\rangle_A \left|I\right\rangle_C\right], \tag{50}$$

where $\big|I\big\rangle_C = \big|l_1 \dots l_d\big\rangle_C$ is a multi-index labeling for basis states of the completely symmetric subspace of $(k-1)$ photons in d modes. Note that k was relabeled as $k+1$ so in comparison with Eq. (49) we now have $k = \sum_{i=1}^{d} l_{I,i} + 1$. A ket $\big|I^{(i)}\big\rangle_A$ differs from $\big|I\big\rangle_C$ by having $l_{I,i}+1$ instead of $l_{I,i}$ in the i-th place, that is, $\big|I^{(i)}\big\rangle_A = \big|l_{I,1} \dots l_{I,i}+1 \dots l_{I,d}\big\rangle_A$. The interpretation is that the A subsystem contains k photons in d modes. The presence of the index I is crucial since the value of $l_{I,i}$ indeed depends on which $\big|I\big\rangle_C$ was used to generate the corresponding $\big|I^{(i)}\big\rangle_A$.

Example. For $d=3$ and $k=2$ the basis consists of the states $\big\{\, \big|I\big\rangle_C \,\big\} = \big\{\, \big|001\big\rangle, \big|010\big\rangle, \big|100\big\rangle \,\big\}$ corresponding to a single photon in three possible modes of the A subsystem. For $\big|100\big\rangle_C$ we get $\big\{\, \big|I^{(i)}\big\rangle_A \,\big\}_{i=1}^{3} = \big\{\, \big|200\big\rangle, \big|110\big\rangle, \big|101\big\rangle \,\big\}$ with the coefficient $l_{I,i}+1$ equal to $2, 1$ and 1, respectively. If we chose a different $\big|I\big\rangle_C$ the result would in general be a different set of vectors and coefficients.

Example. For another example we choose $d=4$ and $k=3$. The basis of the C subsystem consists of the states

$$\big\{\, \big|I\big\rangle_C \,\big\} = \big\{\, \big|0002\big\rangle, \big|0020\big\rangle, \big|0200\big\rangle, \big|2000\big\rangle, \big|0011\big\rangle, \big|0101\big\rangle, \big|0110\big\rangle, \big|1001\big\rangle, \big|1010\big\rangle, \big|1100\big\rangle \,\big\}$$

This corresponds to two photons in four possible modes of the A subsystem. For $\big|0200\big\rangle_C$ we get $\big\{\, \big|I^{(i)}\big\rangle_A \,\big\}_{i=1}^{4} = \big\{\, \big|1200\big\rangle, \big|0300\big\rangle, \big|0210\big\rangle, \big|0201\big\rangle \,\big\}$ with the coefficient $l_{I,i}+1$ equal to $1, 3, 1$ and 1, respectively.

We conclude this section by providing a quantum-optical interpretation of Eq. (43). In this setting the situation is conceptually simpler than the Unruh effect since the issue with non-equivalent Hilbert spaces does not arise. This is indicated by an isometric identification of the input and output Hilbert space in Eq. (43) (the identical labels on the LHS and RHS). Consider an array of d two-mode optical squeezers each described by the unitary operation of Eq. (42). The overall action is described by Eq. (45) since all the input C-modes (the environment) contain vacuum. The total number of photons in the input A-mode equals one and the input pure state can be described by an arbitrary superposition of d modes as in Eq. (44). The squeezing parameter r is common for all squeezing transformations and is analogous to the proper acceleration of the Rindler observer. Simpler constructions of this kind were previously investigated in connection with quantum optical amplifiers [11, 14].

3.2 The structure of the output density matrix and the irreducible representations of $\mathsf{sl}(d,\mathbb{C})$

We will show that the terms appearing in the output density matrix live in spaces that carry representations of $\mathsf{sl}(d,\mathbb{C})$ and the states themselves can be written in terms of the Lie algebra elements.

We begin with a formal definition of the qudit Unruh channel.

Definition 11. The qudit Unruh channel $\mathcal{E}$ is the quantum channel defined by $\mathcal{E}(\psi_A) = \mathrm{Tr}_C\, U\psi_{AC}U^\dagger$ where $U = \bigotimes_{i=1}^{d} U_{A_iC_i}$ with $U_{A_iC_i}$ given by Eq. (45). The action of the channel on an input qudit state Eq. (44) is given by

$$\mathcal{E} : \psi_A \mapsto \sigma_A = (1-z)^{d+1} \bigoplus_{k=1}^{\infty} z^{k-1} \sigma_A^{(k)}, \tag{51}$$

where

$$\begin{aligned} \sigma_A^{(k)} = &\sum_I \sum_{i=1}^{d} |\beta_i|^2 (l_{I,i}+1) \big|I^{(i)}\big\rangle\big\langle I^{(i)}\big|_A \\ &+ \sum_I \sum_{\substack{i,j=1 \\ i\neq j}}^{d} \beta_i \bar{\beta}_j \sqrt{(l_{I,i}+1)(l_{I,j}+1)} \big|I^{(i)}\big\rangle\big\langle I^{(j)}\big|_A, \end{aligned} \tag{52}$$

and we have defined $z = \tanh^2 r$ so that $\cosh^2 r = 1/(1-z)$.

Remark. From Eq. (52) we find that $\sigma_A^{(k)}$ has $\binom{d+k-1}{k}$ rows and columns, while $\mathrm{Tr}\, \sigma_A^{(k)} = \binom{d+k-1}{d}$, which leads to $\mathrm{Tr}\, \sigma_A = 1$. Note also that the letters A and C are used for labelling both the input and output systems.

In summary, the qudit Unruh channel is a map transforming states prepared in a limited sector of the Minkowski observer's Hilbert space (the observer we have called Alice) to the Hilbert space associated with a uniformly accelerating observer (Rindler observer Eve).

Theorem 12. Let λ_α be the generators of the $\mathsf{sl}(d,\mathbb{C})$ Lie algebra in the Chevalley-Serre basis (defined in Appendix A). We write $\lambda_\alpha^{(k)}$ for the matrix representation of λ_α in the kth completely symmetric representation. There exist numbers n_α, *that are independent of* k, such that each block of the output density matrix σ_A can be written in the form

$$\sigma_A^{(k)} = \frac{1}{d}\Big(k\mathbb{I} + \sum_{\alpha=1}^{L} n_\alpha \lambda_\alpha^{(k)}\Big). \tag{53}$$

In particular the first block of σ_A in Eq. (51) can be written as

$$\sigma_A^{(1)} = \frac{1}{d}\Big(\mathbb{I} + \sum_{\alpha=1}^{L} n_\alpha \lambda_\alpha^{(1)}\Big), \tag{54}$$

where $\lambda_\alpha^{(1)}$ are generators of the fundamental representation of the $\mathsf{sl}(d,\mathbb{C})$ algebra defined in the appendix and $L = 2d(d-1)$.

Remark. The set of generators is overcomplete since, for all $d \geq 2$, one has $L = 2d(d-1) > d^2 - 1 = \dim \mathsf{sl}(d,\mathbb{C})$ so there is not an unique expansion of σ_A; however, the theorem asserts that there is *a particular choice* of the expansion coefficients such that

the same coefficients can be used for all the blocks; these will be described explicitly in the proof. The use of this overcomplete set of $\mathsf{sl}(d,\mathbb{C})$ algebra generators will make it easier to identify the components of Eq. (53) with the $\mathsf{sl}(d,\mathbb{C})$-algebra generators for all k. It is more convenient than working with a basis but not essential.

Remark. The blocks $\sigma_A^{(k)}$ are generally not normalized. The factor multiplying the identity in Eq. (53) comes from the ratio $\operatorname{Tr}\mathbb{I}/\operatorname{Tr}\sigma_A^{(k)} = \binom{d+k-1}{k}/\binom{d+k-1}{d} = d/k$.

The proof of Theorem 12 will be split into two lemmas. Lemma 14 will handle the diagonal coefficients of Eq. (53) and Lemma 15 will address the off-diagonal coefficients. The formalism that we use is called the boson operator formalism or boson calculus.

This is a convenient algebraic formalism that relates the matrices that arise from the representations of $\mathsf{sl}(d,\mathbb{C})$ with the boson annihilation and creation operators. Since bosons are invariant under the action of permutations, the boson algebra is well adapted to describing the completely symmetric representations that we care about. The presentation here follows the exposition in the text by Gilmore [26].

If one is working with $n \times n$ matrices then one introduces n independent commuting pairs of boson creation $a_i^\dagger$ and annihilation a_i operators. These obey the commutation rule

$$[a_i, a_j^\dagger] = \delta_{ij} I$$

where I is the identity operator of the algebra generated by the boson operators. Given a matrix A we define a corresponding bilinear operator $\hat{A}$ by the rule

$$\hat{A} = \sum_{ij} a_i^\dagger A_{ij} a_j.$$

An elementary calculation shows that

$$[\hat{A}, \hat{B}] = \widehat{[A, B]}$$

where the bracket on the left is the commutator in the boson algebra and the one on the right is the ordinary commutator of matrices.

This correspondence shows that the commutators of the matrices are faithfully represented by the commutators of the operators; note, however, that the correspondence does not respect ordinary multiplication. Thus, given the commutation relations of a Lie algebra, we can hope to represent them using appropriate combinations of boson operators. In fact, such a correspondence works for all the $\mathsf{sl}(d,\mathbb{C})$ algebras and for some other classes of Lie algebras as well. This was originally discovered by Jordan and rediscovered several years later by Schwinger in the case of $\mathsf{sl}(2,\mathbb{C})$, where it is called the Schwinger oscillator representation of angular momentum.

With these notations in place we have the following theorem whose proof is a routine calculation.

Theorem 13 (See [26])**.** Let $a_1, a_1^\dagger, \ldots, a_d, a_d^\dagger$ be d pairs of operators obeying the canonical commutation relations for bosonic annihilation and creation operators. Then for $1 \leq l, m \leq d$, the following operators

$$\widehat{H_{ml}} = a_m^\dagger a_m - a_l^\dagger a_l \tag{55a}$$

$$\widehat{E_{ml}} = a_m^\dagger a_l \tag{55b}$$

$$\widehat{E_{ml}^\dagger} = a_l^\dagger a_m, \tag{55c}$$

obey the commutation relations of the $\mathsf{sl}(d, \mathbb{C})$ algebra. That is, the operators satisfy the commutation relations (96) from the appendix.

The operator

$$\widehat{\mathbb{I}} \stackrel{\text{def}}{=} \sum_{i=1}^{d} a_i^\dagger a_i, \tag{56}$$

commutes with all the operators from Eqs. (55); it is the operator corresponding to an identity matrix and it is also the operator representing an identity from Eq. (54) for all d.

The above correspondence is well adapted to dealing with the abstract Lie algebra itself and hence with the fundamental representation. This corresponds to the case where there is one photon in one of d modes: in the boson operator form we see that there is exactly one pair of boson operators for each mode. The completely symmetric representations corresponding to higher k require a mild generalization of the correspondence between matrices and boson operators where we have higher-index tensors instead of matrices.

Let $a_1, a_1^\dagger, \ldots, a_d, a_d^\dagger$ be d pairs of operators obeying the canonical commutation relations for bosonic annihilation and creation operators. Suppose that V is the fundamental representation of $\mathsf{sl}(d, \mathbb{C})$; hence it is a vector space carrying a d-dimensional representation of $\mathsf{sl}(d, \mathbb{C})$. Let $e_1, \ldots, e_d$ be the basis vectors in some basis for V. Then the basis vectors of the representation formed by the completely symmetrized k-fold tensor product of V will be labeled by indices $1 \leq i_1 \ldots, i_k \leq d$. The action of the $\mathsf{sl}(d, \mathbb{C})$ Lie algebra elements will be given by tensors with $2k$ indices $1 \leq i_1 \ldots, i_k, j_1, \ldots, j_k \leq d$. The first k indices are completely symmetrized and the next k are also completely symmetrized. Then we make the following correspondence between operators and tensors A (acting on the completely symmetric representation)

$$A_{i_1,\ldots,i_k,j_1,\ldots,j_k} \mapsto \sum_{i_1,\ldots,i_k,j_1,\ldots,j_k} a_{i_1}^\dagger \ldots a_{i_k}^\dagger A_{i_1,\ldots,i_k,j_1,\ldots,j_k} a_{j_1} \ldots a_{j_k}. \tag{57}$$

The introduced notation makes it easy to write a bosonic representation of an identity from Eq. (53). The corresponding tensor is $A_{i_1,\ldots,i_k,j_1,\ldots,j_k} = \delta_{i_1 j_1} \ldots \delta_{i_k j_k}$ and it takes the form of a $\binom{d+k-1}{k}$-dimensional matrix with ones on the diagonal and zeros everywhere else.

To help the reader more easily follow the upcoming lemmas, we provide some examples which illustrate how Eq. (50) leads to the block diagonal structure of the output density matrix of Eq. (52).

Example. For $k = 1$ and an arbitrary d we get from Eq. (50)

$$\sum_I \left[\sum_{i=1}^{d} \beta_i \sqrt{l_{I,i}+1} \left|I^{(i)}\right\rangle_A \left|I\right\rangle_C \right] = \left(\beta_1 \left|1\dots0\right\rangle_A + \beta_2 \left|01\dots0\right\rangle_A + \dots + \beta_d \left|0\dots1\right\rangle_A\right) \left|vac\right\rangle_C . \quad (58)$$

Example. Let $d = 3$ and $k = 3$. Picking up the relevant part of Eq. (50) gives

$$\begin{aligned}\sum_I \left[\sum_{i=1}^{d} \beta_i \sqrt{l_{I,i}+1} \left|I^{(i)}\right\rangle_A \left|I\right\rangle_C \right] &= \Big[\left(\beta_1 \left|102\right\rangle_A + \beta_2 \left|012\right\rangle_A + \beta_3\sqrt{3} \left|003\right\rangle_A\right) \left|002\right\rangle_C \\ &+ \left(\beta_1 \left|120\right\rangle_A + \beta_2\sqrt{3} \left|030\right\rangle_A + \beta_3 \left|021\right\rangle_A\right) \left|020\right\rangle_C \\ &+ \left(\beta_1\sqrt{3} \left|300\right\rangle_A + \beta_2 \left|210\right\rangle_A + \beta_3 \left|201\right\rangle_A\right) \left|200\right\rangle_C \\ &+ \left(\beta_1 \left|111\right\rangle_A + \beta_2\sqrt{2} \left|021\right\rangle_A + \beta_3\sqrt{2} \left|012\right\rangle_A\right) \left|011\right\rangle_C \\ &+ \left(\beta_1\sqrt{2} \left|201\right\rangle_A + \beta_2 \left|111\right\rangle_A + \beta_3\sqrt{2} \left|102\right\rangle_A\right) \left|101\right\rangle_C \\ &+ \left(\beta_1\sqrt{2} \left|210\right\rangle_A + \beta_2\sqrt{2} \left|120\right\rangle_A + \beta_3 \left|111\right\rangle_A\right) \left|110\right\rangle_C \Big]. \quad (59)\end{aligned}$$

Lemma 14. The diagonal part of Eq. (53) can be written as a sum of the diagonal generators of the k-th completely symmetric representation of $\mathsf{sl}(d, \mathbb{C})$ algebra as specified by Theorem 12, and for a given d the coefficients n_α of the diagonal algebra generators can be chosen independently of the representation.

Proof. **Case** $k = 1$. Eq. (58) from the first example makes it clear that the diagonal part of $\sigma_A^{(1)}$ can be written as

$$\sum_{i=1}^{d} |\beta_i|^2 \left|0\dots1_i\dots0\right\rangle \left\langle 0\dots1_i\dots0\right|, \quad (60)$$

where the 1 appears in the ith position. Now the matrix $|0\dots1_i\dots0\rangle\langle0\dots1_i\dots0|$ under the boson correspondence gives the operator $a_i^\dagger a_i$. It therefore suffices to rewrite $a_i^\dagger a_i$ using the boson algebra and then transform back to matrices. We will do the case where $i = 1$ since other values of i are identical up to cyclic permutations of the indices:

$$a_1^\dagger a_1 = \frac{1}{d}\Big(\sum_{k=1}^{d} a_k^\dagger a_k + \sum_{j=1}^{d-1} (a_1^\dagger a_1 - a_{1+j}^\dagger a_{1+j}) \Big) = \frac{1}{d} \left(\widehat{\mathbb{I}} + \sum_{j=1}^{d-1} \widehat{H_{1,1+j}} \right). \quad (61)$$

Now we get back to the matrix form by "removing the hats", i.e. we have

$$|1\dots0\rangle\langle1\dots0| = \frac{1}{d} \left(\mathbb{I} + \sum_{j=1}^{d-1} H_{1,1+j} \right). \quad (62)$$

Note that we have all generators of the form H_{ij} with $i \neq j$, so there are $d(d+1)$ distinct such generators used in the expansion. Taking into account the β coefficients we see that $(d-1)$ of the n_α are just $|\beta_i|^2$ for $i = 1, \ldots, d$.

Remark. The diagonal generators of the form $H_{i,i+1}$, with $\widehat{H_{i,i+1}} = a_i^\dagger a_i - a_{i+1}^\dagger a_{i+1}$, correspond to the simple roots of the fundamental representation introduced in the appendix while the rest are their linear combinations. As mentioned earlier, because of the use of a linearly dependent set of diagonal generators, the expansion coefficients are not uniquely determined. However, for the explicit choice of expansion coefficients and generators given here, the coefficients are independent of the representation.

Case $k > 1$.

It can be readily observed that squaring the coefficient accompanying β_i gives the label of the i-th ket of the A subsystem. So whatever combination leads to the diagonal part corresponding to β_1 will lead after a suitable simple modification to the diagonal part corresponding to β_i.

Using the form of the diagonal generators of $\mathsf{sl}(d, \mathbb{C})$ in the Chevalley-Serre basis (presented in the appendix) we may conclude certain general things about the form of the representations of the diagonal operators in the completely symmetric representations for all k in Eq. (52). Recall that in the geometric picture of the root space each line of the root space diagram is some embedded representation of the $\mathsf{sl}(2, \mathbb{C})$ algebra. Following the construction of higher completely symmetric representations out of the representations of the $\mathsf{sl}(2, \mathbb{C})$ algebras (see Appendix B) we conclude that the vertex coordinates of the k-th representation of $\mathsf{sl}(d, \mathbb{C})$ are scaled by a factor of k as we go to higher k. Therefore, at least for the vertex points of the k-th representation, we can use the same relation as Eq. (62) except that it is scaled by k.

We proceed as with the case $k = 1$ and first consider the term $k|\beta_1|^2|k\,0\ldots0\rangle\langle k\,0\ldots0|$. In the root space diagram this is a vertex of the simplex describing the representation. We can write the tensor $|k\,0\ldots0\rangle\langle k\,0\ldots0|$ as $A^{(11)}$, which is a $2k$-index tensor with 1 whenever the (i_q, j_q) index pair is $(1,1)$ (which happens k times) we see that the boson operator corresponding to this tensor is

$$k|\beta_1|^2 \sum_{i_1,\ldots,i_k,j_1,\ldots,j_k=1}^{d} a_{i_1}^\dagger \ldots a_{i_k}^\dagger A^{(11)}_{i_1,\ldots,i_k,j_1,\ldots,j_k} a_{j_1} \ldots a_{j_k}.$$

Using the form of $A^{(11)}$ we can simplify this expression and use the boson algebra to calculate as follows

$$k|\beta_1|^2 (a_1^\dagger)^k (a_1)^k = \frac{|\beta_1|^2}{d}\Big(k\sum_{i=1}^{d}(a_i^\dagger)^k(a_i)^k + k\sum_{j=1}^{d-1}(a_1^\dagger)^k(a_1)^k - (a_{j+1}^\dagger)^k(a_{j+1}^k)\Big). \quad (63)$$

We see that these are exactly the operator analogues of the representation of the diagonal generators in the higher k representations and we have the same coefficients as we had in the $k = 1$ case. The terms corresponding to the other vertices in the root diagram are handled exactly the same way.

We now have to deal with the rest of the diagonal terms which do not correspond to vertices of the root space diagram. A typical such (diagonal) term is of the form

$$(l_{I,i}+1)|\beta_i|^2|I^{(i)}\rangle\langle I^{(i)}|.$$

Using the transformation from tensors to boson operators given in Eq. (57) we get

$$(k-l)|\beta_i|^2\prod_{i=1}^{d}(a_i^\dagger)^{k_i}\prod_{i=1}^{d}(a_i)^{k_i},$$

where the factor $(k-l)$ is $(l_{I,i}+1)$ where l is the number of steps along the lattice from the vertex state. Now we trivially have

$$(k-l)|\beta_i|^2\mathbb{A}^{[k_i]}=\frac{|\beta_i|^2}{d}\Big(k\mathbb{A}^{[k_i]}+k(d-1)\mathbb{A}^{[k_i]}-ld\mathbb{A}^{[k_i]}\Big), \tag{64}$$

where we have used the abbreviation

$$\mathbb{A}^{[k_i]}=\prod_{i=1}^{d}(a_i^\dagger)^{k_i}\prod_{i=1}^{d}(a_i)^{k_i}.$$

We now argue that these terms are the boson operators corresponding to the generators of the Lie algebra in the completely symmetric representation. The states adjacent to the vertex state $\big|k\,0\ldots0\big\rangle$ are all states of the form $\big|k-1\ldots\big\rangle$. Recall that these states lie on a regular lattice, each segment of which is parallel to one of the (not necessarily simple) roots. We first consider the neighboring state of the form $\big|k-1\,1\ldots0\big\rangle$.

Using the standard coordinate system of the root space diagram, we see that to move to this state means to subtract two from the coordinate parallel to the segment connecting $\big|k\,0\ldots0\big\rangle$ and $\big|k-1\,1\ldots0\big\rangle$ and one from $(d-2)$ other coordinates, since 1 is the projection of the segment on to the remaining $(d-2)$ axes. To get to the rest of the states of the form $\big|k-l\,l\ldots0\big\rangle$, which are further away, we repeat the procedure l times. Noting that $l(-2-(d-2)\times1)=-ld$ we get from Eq. (63)

$$\frac{|\beta_1|^2}{d}\Big(k\mathbb{A}^{[k_i]}+k(d-1)\mathbb{A}^{[k_i]}-ld\mathbb{A}^{[k_i]}\Big). \tag{65}$$

This is exactly what we had in Eq. (64).

The argument for Eq. (65) holds for any state $\big|k-l\ldots\big\rangle$ lying in the interior of the simplex describing the lattice of points in the root space diagram. We first observe that all states of the form $\big|k-l\ldots\big\rangle$ lie l segments away from the vertex point $\big|k\,0\ldots0\big\rangle$ and thus lie on a single hyperplane and are equidistant from the state $\big|k\,0\ldots0\big\rangle$. To get to any of the states on this hyperplane from the vertex we always travel l segments of length two. To reach all these points one does not, of course, traverse segments that are all pointing in the same direction but each segment is parallel to one of the coordinates axes of the root space. Clearly, also in this case, there will be $(d-2)$ projections of

length one to the remaining (non-parallel) coordinates for each segment. There may be multiple paths from a vertex to a given state but this does not affect the argument, which applies to any of the shortest paths.

We conclude that when going from $k = 1$ to $k > 1$ the coefficients $n_\alpha = |\beta_1|^2$ remain the same for the $(d-1)$ diagonal generators from Eq. (53). Again the symmetry of the expression shows that the same argument works with all the β_i. ■

The diagonal terms of σ_A are expressed in terms of the H_{ij} diagonal generators of $\mathsf{sl}(d, \mathbb{C})$. The off diagonal terms will correspond to the step operators of the form E_{ij}. In the previous proof we have been careful to distinguish between the matrix or tensor describing an element of a representation and the boson operator corresponding to it. This correspondence should be clear now and in the next lemma we will just pretend that the boson operators *are* the generators of the Lie algebra in the representation. This will avoid having to insert and remove hats as we did in the last lemma when we were trying to keep the distinction clear.

Lemma 15. The off-diagonal part of Eq. (53) is a sum of $\mathsf{sl}(d, \mathbb{C})$ step operators in the k-th completely symmetric representation as specified in Theorem 12 and, for a given d, the off-diagonal algebra generator coefficients n_α are independent of the representation.

Proof. **Case** $k = 1$. As we discuss in the appendix the step operators of the $\mathsf{sl}(2, \mathbb{C})$ subalgebra correspond to the edges of complete graphs with states $\left|0 \dots 1_l \dots \right\rangle$ occupying the vertices. Starting at the l-th vertex we can see that the bosonic step operator from Theorem 13 takes us to the m-th vertex

$$a_m^\dagger a_l \left|0 \dots 1_l \dots \right\rangle = \left|0 \dots 1_m \dots \right\rangle.$$

Choosing all possible edges (all coefficients $\beta_l \bar{\beta}_m$) we can fully describe the off-diagonal part of the density matrix corresponding to Eq. (58):

$$\sum_{\substack{m,l=1 \\ m<l}}^{d} \beta_l \bar{\beta}_m a_m^\dagger a_l + h.c. \tag{66}$$

There are $d(d-1)$ summands in total and we see that

$$n_\alpha = \beta_l \bar{\beta}_m,$$

where $\alpha = (l, m), l \neq m$.

Remark. The raising operators of the form $a_{l+1}^\dagger a_l$ precisely correspond to the step operators of the fundamental representation written in the Chevalley-Serre basis (the E_{lm}s) introduced in the appendix.

Case $k > 1$. Following the strategy from the case $k = 1$ we choose a particular direction from the l-th to the m-th vertex by setting the coefficients $\beta_i \bar{\beta}_j$ where $(i, j) \neq (l, m)$ to zero. Using basic facts from the appendix and the observation that to get from one vertex

state to the other, one has to pass over $k-1$ intermediate states lying on the connecting edge. These states divide the edge into k segments. So we have to apply the step operator $a_m^\dagger a_l$ k-times. Now we consider the other lines parallel to the edge under consideration. The only difference is that the number of segments is less than k so the step operators have to be applied fewer times. But these are precisely the higher-dimensional step operators written in the bosonic representation.

From Eq. (52) we see that each pair of neighboring states (no matter on which line parallel to the edge under consideration they lie) have the following coefficient

$$\beta_l \bar{\beta}_m \sqrt{(l_{I,l}+1)(l_{I,m}+1)} \big| I^{(l)} \big\rangle\!\big\langle I^{(m)} \big|.$$

However, using the rules for bosonic creation and annihilation operators we find that

$$a_m^\dagger a_l \left| I^{(l)} \right\rangle = \sqrt{l_{I,l}+1}\sqrt{l_{I,m}+1} \left| I^{(m)} \right\rangle. \tag{67}$$

We again conclude that in the transition from $k=1$ to $k>1$ the expansion coefficients in Eq. (53) remain identical

$$n_\alpha = \beta_l \bar{\beta}_m,$$

where $\alpha = (l,m), l \neq m$. ■

Proof of Theorem 12. Putting together Lemmas 14 and 15 capturing separately the diagonal and off-diagonal parts of Eq. (53) gives the theorem statement. The total number of operators is indeed $L = 2d(d-1)$ where $d(d-1)$ of them comes from the diagonal part (see Eqs. (61) and (63) and note that we repeat the procedure d-times). The remaining $d(d-1)$ operators come from the off-diagonal part (Eq. (66) for $k=1$). For $k>1$ the only difference is that we act with all $d(d-1)$ operators from Eq. (66) k-times as witnessed in Eq. (67). ■

Remark. In the last paragraph of Appendix B, we discuss why the generators constructed above are indeed generators of the k-th completely symmetric representation of $\mathsf{sl}(d,\mathbb{C})$, in particular, why they satisfy the necessary commutation relations.

We have seen that the Hilbert spaces carry representations of $SU(d)$; we now show that the transformations effected by the Unruh channel mesh properly with the group actions on the state spaces: the qudit Unruh channel is $SU(d)$-*covariant*. This property is very helpful in evaluating is regular and private quantum capacities. Recall that $\mathcal{DM}(\mathcal{H})$ stands for the space of density matrices on the Hilbert space $\mathcal{H}$.

Definition 16. Let G be a group, $\mathcal{H}_{in}, \mathcal{H}_{out}$ be Hilbert spaces and let $r_1 : G \to GL(\mathcal{H}_{in}), r_2 : G \to GL(\mathcal{H}_{out})$ be two unitary representations of the group G. Let $\mathcal{K} : \mathcal{DM}\big(\mathcal{H}_{in}\big) \to \mathcal{DM}\big(\mathcal{H}_{out}\big)$ be a channel. We say that $\mathcal{K}$ is **covariant with respect to** G and the representations r_1, r_2, if

$$\mathcal{K}\left(r_1(g)\rho r_1(g)^\dagger\right) = r_2(g)\mathcal{K}(\rho)r_2(g)^\dagger \tag{68}$$

holds for all $g \in G, \rho \in \mathcal{DM}(\mathcal{H}_{in})$.

The covariance of the qudit Unruh channel is an easy consequence of the main structure theorem.

Corollary 17. The qudit Unruh channel is $SU(d)$-covariant for the fundamental representation in the input space and any of the completely symmetric representations carried by the output space of the channel.

Proof. The channel output σ_A in Eq. (51) is an infinite-dimensional block-diagonal trace class matrix. It can be rewritten as

$$\sigma_A = \bigoplus_{k=1}^{\infty} s_k \tilde{\sigma}_A^{(k)}, \tag{69}$$

where $s_k = (1-z)^{d+1} z^{k-1} \binom{d+k-1}{d}$. $\tilde{\sigma}_A^{(k)}$ is proportional to $\sigma_A^{(k)}$ such that $\operatorname{Tr} \tilde{\sigma}_A^{(k)} = 1$ for all k. This implies that the qudit Unruh channel can be written as $\mathcal{E}(\psi_A) = \bigoplus_{k=1}^{\infty} s_k \mathcal{E}_k(\psi_A)$, where the $\mathcal{E}_k(\psi_A)$ can be read off Eq. (51). Suppose that $\psi_A \mapsto \psi'_A = r_1(g)\psi_A r_1(g)^\dagger$ for r_1 the defining representation of $SU(d)$ on the multi-rail qudit encoding space. Then

$$\psi_A = \frac{1}{d}\Big(\mathbb{I} + \sum_{\alpha=1}^{L} n_\alpha \lambda_\alpha^{(1)}\Big) \quad \text{and} \quad \psi'_A = \frac{1}{d}\Big(\mathbb{I} + \sum_{\alpha=1}^{L} n'_\alpha \lambda_\alpha^{(1)}\Big) \tag{70}$$

for some choices of n_α and n'_α. Consider the map taking

$$\sigma_A^{(k)} = \frac{1}{d}\Big(k\mathbb{I} + \sum_{\alpha=1}^{L} n_\alpha \lambda_\alpha^{(k)}\Big) \quad \text{to} \quad \sigma_A^{\prime(k)} = \frac{1}{d}\Big(k\mathbb{I} + \sum_{\alpha=1}^{L} n'_\alpha \lambda_\alpha^{(k)}\Big). \tag{71}$$

First we will verify that this map is well-defined despite the fact that the choices of n_α and n'_α are not unique. If $\sum_\alpha n_\alpha \lambda_\alpha^{(1)} = \sum_\alpha m_\alpha \lambda_\alpha^{(1)}$, then this identifies a linear relation in the Lie algebra $\mathsf{sl}(d,\mathbb{C})$ because the $\lambda_\alpha^{(1)}$ are elements of the fundamental representation of $\mathsf{sl}(d,\mathbb{C})$. Any such linear relation must also hold in any representations of $\mathsf{sl}(d,\mathbb{C})$, in particular, the kth completely symmetric representations. It follows that $\sum_\alpha n_\alpha \lambda_\alpha^{(k)} = \sum_\alpha m_\alpha \lambda_\alpha^{(k)}$ so the map is well-defined and, in fact, linear.

The only linear map satisfying Eq. (71), however, is conjugation by $r_2(g)$ where r_2 is k-fold symmetric power of r_1, so we have verified that the following diagram commutes:

$$\begin{array}{ccc} \psi_A & \xrightarrow{\mathcal{E}_k} & \tilde{\sigma}_A^{(k)} \\ {\scriptstyle r_1(g)}\downarrow & & \downarrow{\scriptstyle r_2(g)} \\ \psi'_A & \xrightarrow[\mathcal{E}_k]{} & \tilde{\sigma}_A^{\prime(k)} \end{array}$$

Therefore, the covariance condition Eq. (68) holds for all $\mathcal{E}_k$. Since the output of the qudit Unruh channel is a direct sum of $\mathcal{E}_k(\psi_A)$ we conclude that the qudit Unruh channel is covariant as well. ∎

Remark. We emphasize that the covariance proof shows only that the restriction of the Unruh channel to the input space spanned by input qudit states from Eq. (44) is covariant. As a matter of fact, one can easily show that for a general input state the Unruh channel is not covariant with respect to $SU(d)$.

4 Quantum capacities of the qudit Unruh channel

While there is no known single-letter formula for the quantum capacity of a general quantum channel, if a channel has the property of being either degradable or conjugate degradable, the optimized coherent information does give such a formula [21, 8]. It was shown in [9] that the qubit Unruh channel is conjugate degradable. We will show below that this property extends to the qudit Unruh channels. From there, we will calculate the quantum capacity.

Definition 18. A channel $\mathcal{E}$ is **conjugate degradable** if there exists a quantum channel $\check{\mathcal{D}}$, called a **conjugate degrading map**, which degrades the channel to its complementary channel $\mathcal{E}_c$ up to complex conjugation $\mathcal{C}$:

$$\check{\mathcal{D}} \circ \mathcal{E} = \mathcal{C} \circ \mathcal{E}_c. \tag{72}$$

Theorem 19. The qudit Unruh channel $\mathcal{E}$ from Alice to Eve introduced in Def. 11 is conjugate degradable. The explicit transformation to the complementary output is

$$\mathcal{E}_c(\psi_A) = z\bar{\sigma}_A + (1-z)\omega_0, \tag{73}$$

where $\sigma_A = \mathcal{E}(\psi_A)$ and ω_0 is a diagonal state independent of σ_A.

The proof of the theorem will be preceded by two lemmas for which purpose we rewrite Eq. (50) as

$$\left|\sigma\right\rangle_{AC} = (1-z)^{(d+1)/2} \sum_{k=1}^{\infty} z^{(k-1)/2} \left|\sigma^{(k)}\right\rangle_{AC}. \tag{74}$$

Lemma 20. The following relation holds: $\sigma_C^{(2)} = \bar{\sigma}_A^{(1)} + \mathbb{I}$ where $\sigma_C^{(k)} = \mathrm{Tr}_A\, \sigma_{AC}^{(k)}$ and $\sigma_A^{(k)} = \mathrm{Tr}_C\, \sigma_{AC}^{(k)}$.

Proof. We rewrite a part of the state Eq. (74), namely $\left|\sigma^{(2)}\right\rangle_{AC}$, as

$$\left|\sigma^{(2)}\right\rangle_{AC} = \sqrt{2} \sum_{i=1}^{d} \beta_i \left|ii\right\rangle_A \left|i\right\rangle_C + \sum_{\substack{i,j \\ i\neq j}}^{\binom{d}{2}} \left|ij\right\rangle_A \left(\beta_j \left|i\right\rangle + \beta_i \left|j\right\rangle\right)_C, \tag{75}$$

where for the A subsystem $\left|ii\right\rangle_A$ labels a d-mode Fock state where the i-th position is occupied by two photons. $\left|ij\right\rangle_A$ labels a d-mode Fock state where the i-th and j-th positions are occupied by single photons. There are no other possibilities. The C subsystem

is even simpler since $\left|i\right\rangle_C$ just means the i-th position being occupied by a single photon. This labeling has the advantage of having the same form for all d. Tracing over the A subsystem we get

$$\sigma_C^{(2)} = \sum_{i=1}^{d} \left(2|\beta_i|^2 + \sum_{j\neq i}^{d-1} |\beta_j|^2 \right) \left|i\right\rangle\!\left\langle i\right| + \sum_{\substack{i,j \\ i\neq j}}^{\binom{d}{2}} \beta_j \bar{\beta}_i \left|i\right\rangle\!\left\langle j\right|. \tag{76}$$

Applying the normalization condition $\sum_{i=1}^{d} |\beta_i|^2 = 1$ we find

$$\sigma_C^{(2)} = \mathbb{I} + \sum_{i=1}^{d} |\beta_i|^2 \left|i\right\rangle\!\left\langle i\right| + \sum_{\substack{i,j \\ i\neq j}}^{\binom{d}{2}} \beta_j \bar{\beta}_i \left|i\right\rangle\!\left\langle j\right|. \tag{77}$$

Expanding Eq. (74) for $k = 1$ then gives

$$\left|\sigma^{(1)}\right\rangle_{AC} = \sum_{i=1}^{d} \beta_i \left|i\right\rangle_A \left|0\ldots 0\right\rangle_C . \tag{78}$$

(We are abusing a notation a bit by mixing both ket conventions.) By tracing over the C subsystem we get

$$\sigma_A^{(1)} = \sum_{i=1}^{d} |\beta_i|^2 \left|i\right\rangle\!\left\langle i\right| + \sum_{\substack{i,j \\ i\neq j}}^{\binom{d}{2}} \beta_i \bar{\beta}_j \left|i\right\rangle\!\left\langle j\right|. \tag{79}$$

Comparing with Eq. (77) completes the proof. ■

This shows that, at least for $k = 2$, the complementary output is complex conjugated and admixed with a maximally mixed state with respect to some part of the qudit Unruh channel output. Equally importantly, we see that $\sigma_C^{(2)}$ has an algebra generator structure closely related to that of $\sigma_A^{(1)}$.

Lemma 21. The following relation holds for all k: $\sigma_C^{(k+1)} = \bar{\sigma}_A^{(k)} + \mathbb{I}$.

Proof. In Theorem 12 we explicitly showed that even as the size of the underlying representation is increased, the expansion coefficients of σ_A in terms of the Lie algebra generators can be chosen to be independent of the representation. The same is actually true of the C subsystem. If we simply rewrite the core of Eq. (48)

$$\left\{ \frac{1}{\sqrt{l_1!\ldots l_d!}} \bigotimes_{i=1}^{d} \left(a_i^\dagger\right)^{l_i} \otimes \frac{1}{\sqrt{l_1!\ldots l_d!}} \bigotimes_{i=1}^{d} \left(c_i^\dagger\right)^{l_i} \right\}_{\sum l_i + 1 = k} \tag{80}$$

then the left product composed of $a_i^\dagger$ operators generates the A subsystem whose structure has been completely described. But the right product is identical to the left one and

so Theorem 12 is applicable for the C subsystem as well. In other words, taking Eq. (77) we know exactly how any other $\sigma_C^{(k+1)}$ will look like and we may conclude that

$$\sigma_C^{(k+1)} - \mathbb{I} = \bar{\sigma}_A^{(k)}.$$

■

Proof of Theorem 19. Let us explicitly construct the conjugate degrading map, which isn't hard given the relationships we've identified between the output of the qudit Unruh channel and the output of its complementary channel.

$$\sigma_A = (1-z)^{d+1}\left[\sigma_A^{(1)} \oplus z\sigma_A^{(2)} \oplus z^2\sigma_A^{(3)} \oplus \dots\right] \tag{81}$$

$$\sigma_C = (1-z)^{d+1}\left[\left|0\dots0\right\rangle\!\left\langle 0\dots0\right|_C \oplus z\sigma_C^{(2)} \oplus z^2\sigma_C^{(3)} \oplus \dots\right]. \tag{82}$$

We admix the complex conjugated σ_A with a properly chosen diagonal state and use Lemma 21 to get

$$\sigma_C = z\bar{\sigma}_A + (1-z)\omega_0, \tag{83}$$

where $\omega_0 = (1-z)^d\left[\left|0\dots0\right\rangle\!\left\langle 0\dots0\right| \oplus z\mathbb{I} \oplus z^2\mathbb{I} \oplus \dots\right]$. This concludes the proof. ■

If a channel is covariant and conjugate degradable, then the maximization in the formula for the quantum capacity from Theorem 2 is achieved with a maximally mixed input qudit π_A. (See the calculation leading up to Eq. (9) in [8].) The same happens for the evaluation of the formula for the private quantum capacity in Theorem 5. Since we have shown that the qudit Unruh channel is both covariant and conjugate degradable, we must therefore calculate $\mathcal{E}(\pi_A)$ and $\mathcal{E}_c(\pi_A)$.

The image of a single input pure state, say $\left|1\right\rangle$, reads

$$\mathcal{E} : \left|1\right\rangle_A \mapsto (1-z)^{d+1}\bigoplus_{k=1}^{\infty} z^{k-1} \sum_{I^{(1)}} (l_{I,1}+1)\left|I^{(1)}\right\rangle\!\left\langle I^{(1)}\right|_A, \tag{84}$$

where we recall that $(l_{I,1}+1)$ is the first label of $\left|I^{(1)}\right\rangle_A$ for a given k and d. Let $\pi_{1\to i}$ be the permutation transposing 1 and i. For the input ket $\left|i\right\rangle = \pi_{1\to i}\left|1\right\rangle$ we get from Eq. (62)

$$\mathcal{E} : \left|i\right\rangle_A \mapsto (1-z)^{d+1}\bigoplus_{k=1}^{\infty} z^{k-1} \sum_{I^{(i)}} (l_{I,i}+1)\left|I^{(i)}\right\rangle\!\left\langle I^{(i)}\right|_A. \tag{85}$$

Since $\sum_{i=1}^{d}(l_{I,i}+1) = k$ and $\pi_A = 1/d\sum_{i=1}^{d}\left|i\right\rangle\!\left\langle i\right|_A$ we get

$$\mathcal{E} : \pi_A \mapsto \rho_A = \frac{1}{d}(1-z)^{d+1}\bigoplus_{k=1}^{\infty} kz^{k-1} \sum_{I^{(i)}=1}^{\binom{d+k-1}{k}} \left|I^{(i)}\right\rangle\!\left\langle I^{(i)}\right|_A, \tag{86}$$

where the sum over i from π_A is hidden in the sum over $I^{(i)}$. The example from Eq. (59) can be helpful. Observe that, on each irrep, the state is proportional to the identity as

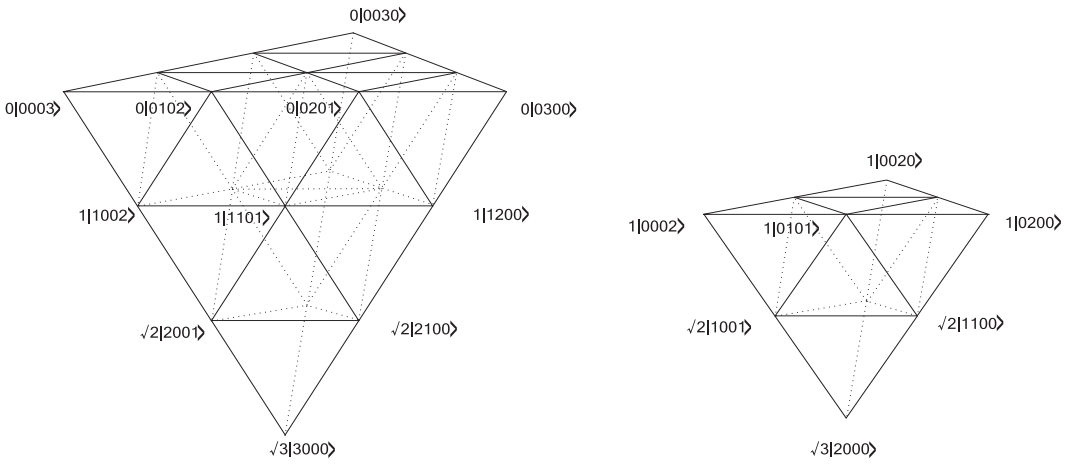

Figure 5: We illustrate the calculation of the image of a maximally input mixed input qudit $\rho_A = \mathcal{E}(\pi_A)$ (on the left) and $\rho_C = \mathcal{E}_c(\pi_A)$ (on the right) on $d = 4$ and $k = 3$. Both plots capture the situation where $\beta_1 = 1$. We can visualize the calculations in Eqs. (86) and (88) if we realize that the permutation $\pi_{1\to i}$ preserves the coefficients $\sqrt{k}$ when acting on $\big|k\,0\ldots\big\rangle$ (on the left) or on $\big|k-1\ldots\big\rangle$ (on the right). The summing procedure $\sum_{i=1}^{d}\big|i\big\rangle\!\big\langle i\big|_A$ is like adding d rotated simplices with squared coefficients.

required by Schur's lemma. The output from the channel complementary to the Unruh channel will also be needed. Once we know the structure of the k-th output block of the Unruh channel Lemma 21, tells us about the structure of the $(k+1)$-th block of its complementary channel. Its dimension must be same and so the states $\big|I\big\rangle_C$ span the $\binom{d+k-2}{k-1}$-dimensional completely symmetric subspace of $(k+1)$ photons. But we prefer to compare the k-th complementary block with the k-th Unruh channel output block because in our notation $\big|I\big\rangle_C$ contains one photon less than $\big|I^{(i)}\big\rangle_A$. It follows from Lemma 21 and Eq. (84) that

$$\mathcal{E}_c : \big|1\big\rangle_A \mapsto (1-z)^{d+1}\bigoplus_{k=1}^{\infty} z^{k-1} \sum_{I=1}^{\binom{d+k-2}{k-1}} (l_{I,1}+1)\big|I\big\rangle\!\big\langle I\big|_C. \tag{87}$$

for $\beta_1 = 1$ and as a result the coefficients $(l_{I,1}+1)$ remain the same. Because the eigenvalues are equal we see that the k-th block of the complementary channel is the complement of the k-th block of the Unruh channel. Fig. 5 shows an example of the relation between two complementary blocks. Since for β_1 the coefficient $(l_{I,1}+1)$ for the 'lowest' states $\big|0\,k\,0\ldots\big\rangle$ equals one, the action of $\pi_{1\to i}$ transfers the coefficient one to the 'highest' state $\big|k\,0\ldots\big\rangle$. This happens exactly $(d-1)$ times (that is, for all remaining β_i's, $i = 2\ldots d$) and so we may conclude that a maximally mixed input qudit

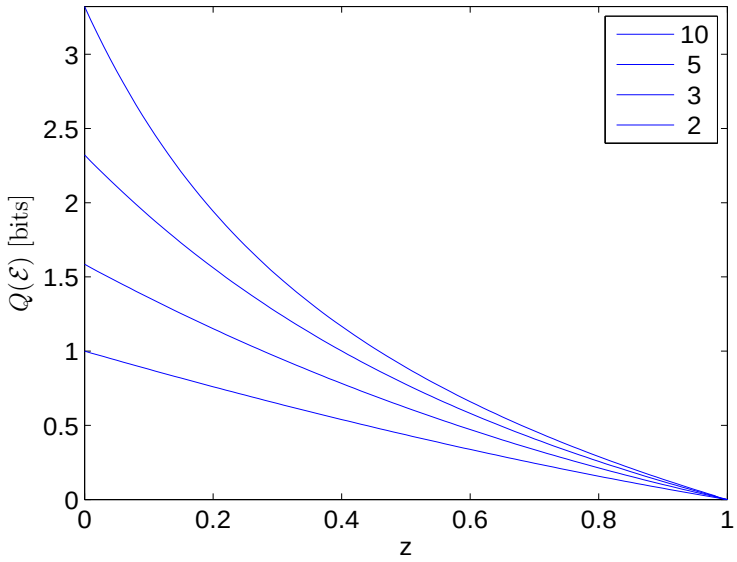

Figure 6: The quantum capacity as calculated by Eq. (91) for several qudit Unruh channels. The curve achieving a capacity of 1 for $z = 0$ corresponds to $d = 2$. The others, in order of increasing quantum capacity, are $d = 3, 5$ and 10.

transforms as

$$\mathcal{E}_c : \pi_A \mapsto \rho_C = \frac{1}{d}(1-z)^{d+1} \bigoplus_{k=1}^{\infty} (d+k-1) z^{k-1} \sum_{I=1}^{\binom{d+k-2}{k-1}} |I\rangle\langle I|_C. \tag{88}$$

Once again, the state is proportional to the identity on each irrep. We will take Eq. (88) as the definition of ρ_C for the remainder of the paper. We define $T_{d,z} = 1/d(1-z)^{d+1}$ and after some straightforward algebra we get

$$H(A)_\rho = -\log T_{d,z} - (1+d)\frac{z}{1-z}\log z - T_{d,z}\sum_{k=1}^{\infty}\binom{d+k-1}{k} k z^{k-1}\log k. \tag{89}$$

Similarly, for the complementary output Eq. (88)

$$\begin{aligned} H(C)_\rho = &-\log T_{d,z} - (1+d)\frac{z}{1-z}\log z \\ &- T_{d,z}\sum_{k=1}^{\infty}\binom{d+k-2}{k-1}(d+k-1)z^{k-1}\log(d+k-1). \end{aligned} \tag{90}$$

The quantum capacity of the qudit Unruh channel simplifies to

$$Q(\mathcal{E}) = H(A)_\rho - H(C)_\rho = T_{d,z}\sum_{k=1}^{\infty}\binom{d+k-1}{k} k z^{k-1}\log\frac{d+k-1}{k}. \tag{91}$$

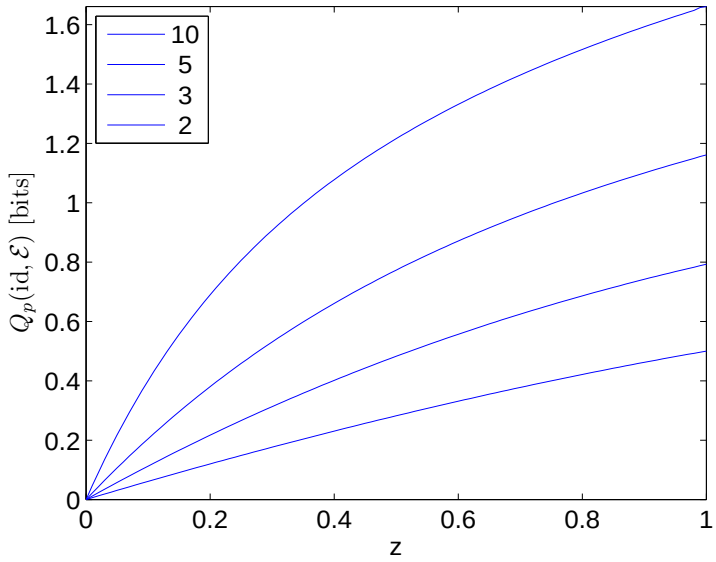

Figure 7: The private quantum capacity as calculated by Eq. (92) for several qudit Unruh channels. In order of increasing capacity, the curves correspond to $d = 2, 3, 5$ and 10.

We present the plot of the quantum capacity as a function of the acceleration parameter in Fig. 6.

For the private quantum capacity we recall our single-letter formula from Theorem 5. The channel to Bob is a noiseless channel and so

$$\begin{aligned} Q_p(\mathrm{id},\mathcal{E}) &= \tfrac{1}{2} I(A';C)_\rho \\ &= \tfrac{1}{2}\big(\log d + H(C)_\rho - H(A)_\rho\big) \\ &= \tfrac{1}{2}\left(\log d - T_{d,z}\sum_{k=1}^{\infty}\binom{d+k-1}{k} k z^{k-1}\log\frac{d+k-1}{k}\right). \end{aligned} \tag{92}$$

The private quantum capacity is plotted in Figs. 7 and 8. The second figure demonstrates that private communication is more efficient with qudit encodings than with qubit encodings even after normalization for the fact that a qudit channel carries more information than a qubit channel when $d > 2$. Therefore, for the qudit Unruh channel more efficient encodings are possible.

5 Conclusions

We investigated two communication problems in Rindler spacetime. The first was to determine the optimal rate at which a sender could reliably transmit qubits to a uni-

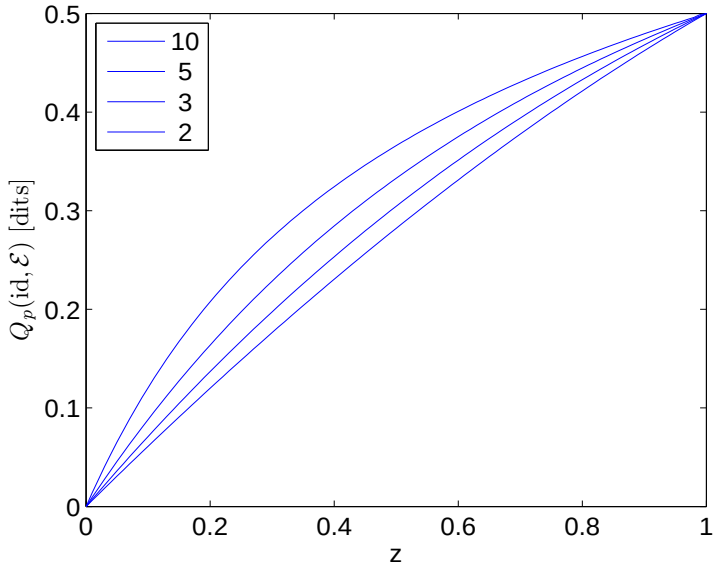

Figure 8: The private quantum capacity given by Eq. (92) for several qudit Unruh channels in units of dits. The uppermost curve corresponds to $d = 10$, then in order $d = 5, 3, 2$. This presentation facilitates comparison of the private quantum capacity for different d by correcting for the fact that a noiseless qudit channel can send $\log d$ times as much information as a noiseless qubit channel. In these units, one immediately sees that in the limit of infinite acceleration, the private quantum capacity approaches a value of $\frac{1}{2} \log d$, meaning that Alice and Bob need only sacrifice half of their transmission bandwidth to secure their messages. More interestingly, the graph indicates that using higher d yields more efficient encodings for finite values of Eve's acceleration.

formly accelerating receiver. While this problem has resisted solution for general quantum channels, in the case of the qudit Unruh channels, we are able to extract a compact, tractable formula which is strictly positive for all accelerations. In order to evaluate the capacity, we decomposed the output of the Unruh channel into irreducible completely symmetric representations of the unitary group. From this decomposition, we were able to show that the channels have a rare and useful property known as conjugate degradability, which makes the calculation of the capacity possible.

The second problem involves securely sending encrypted quantum information from an inertial sender to an inertial receiver in the presence of an accelerating eavesdropper. Because the associated general private quantum capacity problem had only been very briefly discussed previously, we began by studying it for arbitrary channels. In the case where the channel from the sender to the intended receiver is noiseless, our formula "single-letterizes", meaning that it involves no intractable limits. Specifically, the private quantum capacity is equal to the entanglement-assisted capacity to the eavesdropper's

environment. Applied to the qudit Unruh channels, we find the private quantum capacity is positive for all non-zero eavesdropper accelerations, no matter how small.

While we have phrased all our results in the language of Rindler spacetime and accelerating observers, the mathematics also describes the noise induced by a nonlinear optical parametric amplifier (NOPA) [11, 14]. Our quantum capacity result therefore indicates that the quantum capacity through such an amplifier with arbitrarily high gain is always strictly positive and can be exactly calculated.

A natural direction for future study would be to relax some of the assumptions made in this article. First, it would be more natural to impose a power restriction, in the form of the average number of photons per channel use, than to restrict to the d-rail encodings we study here [30]. It would also be interesting to use a more realistic model of the channel from sender to receiver than the noiseless channel studied here. Finally, we have been very conservative in modeling the eavesdropper, allowing her to perform arbitrary operations on her Rindler modes, ignoring her necessarily finite extent. While moving to a power restriction is unlikely to change the qualitative features of our conclusions, there is significant room for new effects when studying realistic receiver and eavesdropper channels. In particular, the quantum capacity would likely vanish at a finite acceleration and the private quantum capacity might only be non-zero for sufficiently high accelerations.

Acknowledgements

We would like to thank Keshav Dasgupta, Alex Maloney and Mark Wilde for helpful discussions. This work was supported by a grant from the Office of Naval Research (N000140811249). We also gratefully acknowledge the support of the Canada Research Chairs program, CIFAR, INTRIQ, MITACS, NSERC, the Perimeter Institute and QuantumWorks.

A Background on representation theory

In the main body of the paper we exploited the covariance of the Unruh channel in order to calculate quantities of interest. This used some standard material on the representation theory of Lie algebras that may not be familiar to all readers. In this section we collect the relevant definitions for the benefit of such a reader.

The representations of any Lie group are closely related to the representations of the corresponding Lie algebra: in physicists' language this amounts to working with the "infinitesimal generators" of the group. Mathematically, a Lie group is a group that is also a smooth manifold with all the group operations being smooth (infinitely differentiable). The Lie algebra is the tangent space at the identity. An easy, but fundamental, result says that associated with any representation of a Lie group is a unique corresponding representation of the Lie algebra and the representation of the Lie group is irreducible if and only if the corresponding Lie algebra representation is irreducible. From the rep-

resentations of the Lie algebra we can reconstruct the representations of the connected component of the identity of the Lie group; so, in particular, if the Lie group is connected the Lie algebra representations determine the Lie group representations.

The Lie algebra of $SU(d)$ is $\mathsf{su}(d)$ and consists of the complex self-adjoint[1] matrices with trace zero. It is more convenient to work with the complexified form which is $\mathsf{su}(d) \otimes \mathbb{C}$. It is easy to see that this is isomorphic to $\mathsf{sl}(d, \mathbb{C})$. Thus we have to classify the representations of $\mathsf{sl}(d, \mathbb{C})$.

The paradigmatic example of the classification of the finite-dimensional representations of a Lie algebra is the case of $\mathsf{sl}(2, \mathbb{C})$. Here there are three generators of the Lie algebra: J_x, J_y, J_z, none of them commute with each other but they all commute with $\mathbf{J}^2 = J_x^2 + J_y^2 + J_z^2$. The irreps are eigenspaces of $\mathbf{J}^2$ and are usually labelled by the corresponding eigenvalue of $\mathbf{J}^2$, or more precisely, by a number that determines the eigenvalue. In this case the label of each irrep is a positive integer j, which is the dimension of the irrep and the eigenvalue is $\frac{1}{4}(j^2 - 1)$. A basis for the irrep is given by the eigenvectors of J_z and the combinations $J^{\pm} = J_x \pm iJ_y$ act as raising and lowering operators. All this is assumed familiar to the reader; the $\mathsf{sl}(d, \mathbb{C})$ case generalizes this situation.

In the $\mathsf{sl}(d, \mathbb{C})$ case there may be several mutually commuting operators instead of just one as in $\mathsf{sl}(2, \mathbb{C})$. A *maximal* commuting set of operators of a (semi-simple) Lie algebra[2] is called a *Cartan subalgebra*. The Cartan subalgebra of $\mathsf{sl}(d, \mathbb{C})$ has dimension $r = d - 1$; we say that the rank of the Lie algebra is r. We write $\mathbf{H} = (H_1, \ldots, H_r)$ for the Cartan subalgebra generated by the elements $\{H_1, \ldots, H_r\}$ of the Lie algebra; these elements are assumed to be linearly independent. Once a Cartan subalgebra has been chosen we can use the common eigenvectors of the members of the Cartan subalgebra as the basis vectors of an irreducible representation just as we used the eigenvectors of J_z in the case of $\mathsf{sl}(2, \mathbb{C})$.

Definition 22. An r-tuple $\alpha = (\alpha_1, \ldots, \alpha_r)$ of complex numbers is called a **root** if: (i) not all the α_i are zero, (ii) there is an element E of $\mathsf{sl}(d, \mathbb{C})$ such that

$$[H_i, E] = \alpha_i E. \tag{93}$$

Typically, we use the root to label E, thus, we would write $[H_i, E_\alpha] = \alpha_i E_\alpha$. A maximally independent set of the form $\{H_i, E_\alpha\}$, where the H_i are a basis of the Cartan subalgebra and the E_α are associated with roots as above, is called a Cartan-Weyl basis [26, 23] of the Lie algebra.

Among all the roots one can choose (nonuniquely) a class of special roots called positive roots.

Definition 23. A set of roots is called a collection of **positive roots** if: (i) for any root α either α or $-\alpha$, but not both are in the set, and (ii) for any roots α, β in the set then if $\alpha + \beta$ is a root it must also be in the set.

[1] We use the convention that the passage from the Lie algebra to the Lie group is $X \mapsto e^{i}X$ rather than $X \mapsto e^{X}$, the latter is common in the pure mathematics literature.

[2] This is not the right definition for general Lie algebras but it is adequate for semi-simple Lie algebras.

Once we have designated a family of roots as positive roots we can define what it means for a root to be simple.

Definition 24. A positive root is called a **positive simple root** if it cannot be written as a linear combination of other positive roots.

Definition 25. If ρ (where $\rho : \mathsf{sl}(d,\mathbb{C}) \to GL(V)$ for some V) is a representation of $\mathsf{sl}(d,\mathbb{C})$ then a r-tuple $\mu = (\mu_1, \ldots, \mu_r)$ of complex numbers is a **weight** for ρ if there is a nonzero vector $\psi \in V$, called a **weight vector**, such that ψ is an eigenvector of each H_i with eigenvalue μ_i.

If μ is a weight and ψ a weight vector for ρ and α is a root then

$$\rho(H_i)\rho(E)\psi = (\mu_i + \alpha_i)\rho(E)\psi. \tag{94}$$

In short, E produces a new weight vector and changes some, perhaps all, of the eigenvalues of the Cartan operators. The root is a vector in the weight space that points in the direction in which the weights are changing. The E operators are called shift or raising and lowering operators; they are the analogues of the $J^{\pm}$ except now there are many of them pointing in different directions. Roughly speaking, the positive roots correspond to raising operators and the negative roots to lowering operators. We classify the irreducible representations by the *highest possible value of the weight*, although doing so of course requires defining a suitable order on the weights.

A special example of a Cartan-Weyl basis is the Chevalley-Serre basis [26, 23]. Two aspects make this basis special: (i) The step operators are associated to simple roots and (ii) the normalization is chosen such that the roots are integers. Unless explicitly stated we work in this basis because it has a useful geometric interpretation.

To give the operators a geometric interpretation we will work with a specific matrix representation of the $\mathsf{sl}(d,\mathbb{C})$ algebra. We define E_{ij}, where $1 \leq i \neq j \leq d$, as the matrix having one where the i-th row and the j-th column intersect and the rest of the entries are zeros. Furthermore we define a diagonal matrix H_{ij} in which the i-th diagonal entry is 1, the j-th diagonal entry is -1 and the rest are zeros. If we assume $j = i + 1$ the set $\{H_{ij}, E_{ij}, E_{ij}^\dagger\}$ forms the Chevalley-Serre basis for $\mathsf{sl}(d,\mathbb{C})$. More explicitly, for $d = 2$ we get

$$H_{12} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{95a}$$

$$E_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \tag{95b}$$

$$E_{12}^\dagger = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}. \tag{95c}$$

It is often the case that one is working with the diagonal matrix $h_{i(i+1)}$ so we often just write H_i for this. For the matrices just defined we have the following commutators:

$$[H_i, E_{ij}] = 2E_{ij} \tag{96a}$$

$$[H_i, E_{ij}^\dagger] = -2E_{ij}^\dagger. \tag{96b}$$

This choice of basis opens the way to a geometric picture based on the so-called root space diagram.

The simple roots are elements of a vector space dual to the one spanned by elements of the Cartan subalgebra. A root α defines a linear map, also written α, on the Cartan subalgebra by the simple rule $\alpha(H_i) = \alpha_i$; since the H_i form a basis for the Cartan subalgebra this gives a linear map. This definition has the property that for a generic H in the Cartan subalgebra and E associated with the root α we have $[H, E] = \alpha(H)E$. Thus we can think of roots as tuples or as elements of the dual space.

This justifies calling the dual space the space of roots. For the $\mathsf{sl}(d, \mathbb{C})$ Lie algebra the space of roots is $(d-1)$-dimensional and the simple root vectors, defined as r-tuples of simple roots, form a basis (which, in general, is not orthogonal). It can be shown that two consecutive simple root vectors subtend the angle $2\pi/3$.

In terms of the Chevalley-Serre basis we can write explicit versions of Eq. (93) and Eq. (94). If we write $\mu = (\mu_1, \ldots, \mu_r)$ for a weight and ψ and for the corresponding weight vector, then we have $H_i\psi = \mu_i\psi$.

We rewrite Eq. (93) as

$$[H_i, E_{ij}] = (\mu_i^{(i)} - \mu_i^{(j)})E_{ij}, \tag{97}$$

where the $\mu_i^{(j)}$ are the possible eigenvalues of H_i; here $\alpha_{ij} = \mu_i^{(i)} - \mu_i^{(j)}$. This shows how the E_{ij} serves as a "step" operator that takes an eigenvector with eigenvalue $\mu_i^{(i)}$ to one with eigenvalue $\mu_i^{(j)}$.

We can write the H_i explicitly in terms of the spectral decomposition:

$$H_i = \sum_{j=1}^{d} \mu_i^{(j)} \big|\psi_j\big\rangle\big\langle\psi_j\big|,$$

where $\big|\psi_j\big\rangle$ is the eigenvector corresponding to the $\mu_i^{(j)}$ of H_i.

Fig. 9a illustrates the situation for $d = 2$ and $d = 3$. Hence for each fundamental representation of $\mathsf{sl}(d, \mathbb{C})$ there are d points each representing an eigenvector $\big|\psi_j\big\rangle$.

The important role played by the (fundamental) weights is that they form the basis for the space of roots and hence they define the coordinates of the eigenvectors in the space of roots. The choices of bases have been made to ensure that all these coordinates are integers.

In the geometric presentation of this data, the different common eigenvectors of the H_i in the fundamental representation are shown as points in a lattice. The step operators E_{ij} define the transitions between these points. All the points of the $\mathsf{sl}(d, \mathbb{C})$ fundamental representations are interconnected. The operator responsible for a transition from site $\big|\psi_i\big\rangle$ to $\big|\psi_j\big\rangle$ is the operator E_{ij} or $E_{ij}^\dagger$ for the opposite direction. It also follows from Eqs. (96) that each segment connecting two neighboring lattice points corresponds to changing exactly one of the coordinates of the lattice point by exactly 2; this just reflects the fact that the lines correspond to representations of $\mathsf{sl}(2, \mathbb{C})$.

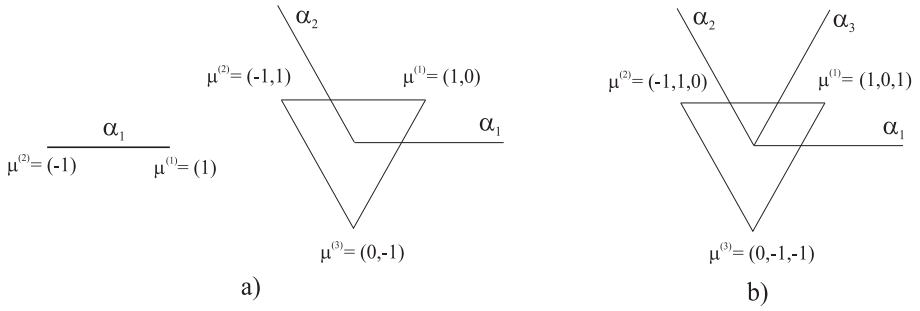

Figure 9: (a) We illustrate the spaces of roots for $\mathsf{sl}(2,\mathbb{C})$ and $\mathsf{sl}(3,\mathbb{C})$. The basis vectors are simple roots and are indicated by α_i. For the weights (vertices) we explicitly write down their coordinates in this basis. We can read off the generators of the Cartan subalgebra from the weights. (b) It is sometimes helpful to introduce an overcomplete basis. The position of α_3 reflects the relation $H_3 = H_1 + H_2$ for H_3 in Eq. (98) and it is not a simple root.

The fundamental representations of $\mathsf{sl}(d,\mathbb{C})$ algebra contain $r = d-1$ linearly independent $\mathsf{sl}(2,\mathbb{C})$ subalgebras each satisfying Eqs. (95). However, since the root space diagram is a complete graph there are in total $\binom{d}{2}$ linearly dependent $\mathsf{sl}(2,\mathbb{C})$ subalgebras corresponding to the number of edges. The analogues of the H_i, i.e. the generators which will be diagonal, of the "additional" $\mathsf{sl}(2,\mathbb{C})$ subalgebras are constructed similarly to the H_i's above. The only difference is that 1 and -1 on the diagonal are separated by one or more zeros. As an example ($d = 3$), the remaining element of the Cartan subalgebra is

$$H_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}. \tag{98}$$

Therefore, the rank of the weight vectors equals three and it corresponds to introducing an overcomplete root basis, see Fig. 9b. Note that H_3 does not correspond to a simple root. Indeed, the axis α_3 in Fig. 9b can be obtained by a linear combination of α_1 and α_2 which are both positive root vectors.

The fundamental representation of $\mathsf{sl}(d,\mathbb{C})$ is a d-dimensional representation with one of the simple roots is assigned 1 and all others are zero. This exactly corresponds to the case where we are looking at the representation corresponding to $k = 1$. This is a d-dimensional space. The other finite-dimensional representations are obtained by forming tensor powers of this representation and symmetrizing and antisymmetrizing parts of the tensor power. We are looking at the completely symmetric representations so the combinatorics are particularly simple. The completely symmetric representations are obtained by taking the completely symmetric tensor powers of the fundamental representation. A well-known elementary argument shows that the dimension of the space is $\binom{d+k-1}{d-1} = \binom{d+k-1}{k}$.

B Geometric picture of the completely symmetric representations of the $\mathsf{sl}(d,\mathbb{C})$ Lie algebras

For the purpose of this article we are interested in particular higher-dimensional representations of $\mathsf{sl}(d,\mathbb{C})$: the completely symmetric representations. The space of roots of $\mathsf{sl}(d,\mathbb{C})$ is $(d-1)$-dimensional and the fundamental root space diagrams are $(d-1)$-simplices. The k-th lowest completely symmetric representations of $\mathsf{sl}(d,\mathbb{C})$ are again $(d-1)$-simplices. We can describe their geometric structure as follows: Each edge connecting a pair of vertices contains $k+1$ equidistant points: these are completely symmetric states $\chi_{j_1} = \psi_{(j_2}\dots\psi_{j_d)}$. The round brackets indicate symmetrization over the indices inside.

Hence the simplex can be divided into k segments each of length two. Any two points are connected provided they lie on a line parallel to an edge. This construction determines a lattice. At each lattice point lies another completely symmetric state. The coordinates are given by a rank $r = d-1$ tensor and they form a higher-dimensional representation of the $\mathsf{sl}(d,\mathbb{C})$ Cartan subalgebra generators. The states of the k-th lowest completely symmetric representation of $\mathsf{sl}(d,\mathbb{C})$ span a $\binom{d+k-1}{k}$-dimensional space. Two spaces of roots are illustrated in Fig. 10.

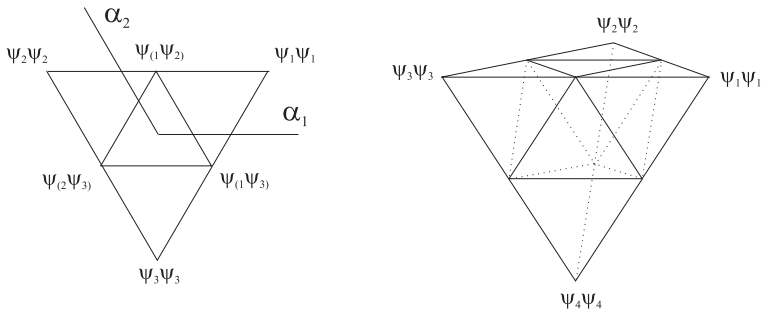

Figure 10: The space of roots for $d=3$ ($k=2$) on the left and $d=4$ ($k=2$) on the right. Let us choose the left plot to illustrate the explicit decomposition into the $\mathsf{sl}(2,\mathbb{C})$ subalgebras. There are two lines parallel to each simple root vector. One line (the edge) has two segments and it is the second lowest representation of $\mathsf{sl}(2,\mathbb{C})$. The single-segment line is the fundamental representation of $\mathsf{sl}(2,\mathbb{C})$. If we direct sum these two algebras and the same thing with those corresponding to α_2 they clearly inherit the commutation relation of the $\mathsf{sl}(2,\mathbb{C})$ algebra. They indeed form the second-lowest completely symmetric representation of $\mathsf{sl}(3,\mathbb{C})$.

All lines of the inner structure connecting the states in the l-th dimensional representations of $\mathsf{sl}(d,\mathbb{C})$ determine the k-th representations of $\mathsf{sl}(2,\mathbb{C})$ for $l = 1\dots k$. These elementary subalgebras serve as building blocks for the generators of the given completely symmetric representation of $\mathsf{sl}(d,\mathbb{C})$. The construction is as follows: For a given edge there is a number of lines parallel to it and so the $\mathsf{sl}(d,\mathbb{C})$ subalgebra generators are

formed by a direct sum of these $\mathsf{sl}(2,\mathbb{C})$ subalgebras. The reason for a direct sum is that they, by construction, act on mutually orthogonal subspaces. Note that it does not imply that the completely symmetric representations of $\mathsf{sl}(d,\mathbb{C})$ are direct sum representations. They are actually irreducible. The direct sum subalgebras that have been created do not themselves span mutually orthogonal subspaces, see Fig. 10 for illustration. The consequence is that the generators constructed in this way manifestly satisfy the commutation relations for $\mathsf{sl}(d,\mathbb{C})$.

For the proof of Lemma 14 we choose a specific coordinate system. The space of roots of $\mathsf{sl}(d,\mathbb{C})$ is $(d-1)$-dimensional and we may choose a (non-orthogonal) coordinate system in many ways. As illustrated in Fig. 9 (b) for $d=3$ we can choose the axes corresponding to any pair $\pm\alpha_i, \pm\alpha_j$ where $i=j=1\ldots3, i\neq j$ and not only the simple roots α_1, α_2. In Lemma 14 we first choose the starting highest weight vector (a vertex state) and then it is advantageous to set up our coordinate system such that the vertex state coordinates are $(k\ldots k)$. As an example, if our vertex state was $\psi_1\psi_1$ in Fig. 10 (on the left) the choice of coordinates would be α_1, α_3 where $\alpha_3=\alpha_1+\alpha_2$ with the state coordinates being (22).

References

[1] R. Ahlswede and I. Csiszar. Common randomness in information theory and cryptography. I. Secret sharing. *IEEE Transactions on Information Theory*, 39(4):1121–1132, 1993.

[2] R. Alicki and M. Fannes. Continuity of quantum conditional information. *Journal of Physics A*, 37(5):L55, 2004.

[3] P. M. Alsing and G. J. Milburn. Teleportation with a uniformly accelerated partner. *Physical Review Letters*, 91(18):180404, 2003.

[4] S.M. Barnett and P.M. Radmore. *Methods in theoretical quantum optics*. Oxford University Press, USA, 1997.

[5] H. Barnum, M. A. Nielsen, and B. Schumacher. Information transmission through a noisy quantum channel. *Physical Review A*, 57:4153–4175, 1998.

[6] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal. Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem. *IEEE Transactions on Information Theory*, 48:10:2637–2655, 2002.

[7] I. Bjelaković, H. Boche, and J. Nötze. Entanglement transmission capacity of compound channels. *arXiv:0904.3011*, 2009.

[8] K. Brádler, N. Dutil, P. Hayden, and A. Muhammad. Conjugate Degradability and the Quantum Capacity of Cloning Channels. *Journal of Mathematical Physics*, 51:072201, 2010.

[9] K. Brádler, P. Hayden, and P. Panangaden. Private information via the Unruh effect. *Journal of High Energy Physics*, 8:74–+, August 2009.

[10] F. G. S. L. Brandão and J. Oppenheim. The quantum one-time pad in the presence of an eavesdropper. *arXiv:1004.3328*, 2010.

[11] S. L. Braunstein, N. J. Cerf, S. Iblisdir, P. Van Loock, and S. Massar. Optimal cloning of coherent states with a linear amplifier and beam splitters. *Physical Review Letters*, 86(21):4938–4941, 2001.

[12] P. Caban and J. Rembieliński. Lorentz-covariant reduced spin density matrix and Einstein-Podolsky-Rosen-Bohm correlations. *Physical Review A*, 72:012103, 2005.

[13] N. Cai, A. Winter, and R. W. Yeung. Quantum privacy and quantum wiretap channels. *Problems of Information Transmission*, 40(4):318–336, 2005.

[14] C. M. Caves. Quantum limits on noise in linear amplifiers. *Physical Review D*, 26(8):1817–1839, 1982.

[15] M. Cliche and A. Kempf. Relativistic quantum channel of communication through field quanta. *Physical Review A*, 81(1):12330, 2010.

[16] L. C. B. Crispino, A. Higuchi, and G. E. A. Matsas. The Unruh effect and its applications. *Reviews of Modern Physics*, 80:787, 2008.

[17] M. Czachor and M. Wilczewski. Relativistic Bennett-Brassard cryptographic scheme, relativistic errors, and how to correct them. *Physical Review A*, 68(1):010302, 2003.

[18] A. Datta. Quantum discord between relatively accelerated observers. *Physical Review A*, 80(5):52304, 2009.

[19] P. C. W. Davies. Scalar production in Schwarzschild and Rindler metrics. *Journal of Physics A: Mathematical and General*, 8:609, 1975.

[20] I. Devetak. The private classical capacity and quantum capacity of a quantum channel. *IEEE Transactions on Information Theory*, 51(1):44–55, 2005.

[21] I. Devetak and P. W. Shor. The capacity of a quantum channel for simultaneous transmission of classical and quantum information. *Communications in Mathematical Physics*, 256(2):287–303, 2005.

[22] J. Doukas and B. Carson. Entanglement of two qubits in a relativistic orbit. *Physical Review A*, 81(6):062320, 2010.

[23] J. Fuchs and C. Schweigert. *Symmetries, Lie algebras and representations: A graduate course for physicists*. Cambridge University Press, 2003.

[24] I. FuentesSchuller and R. B. Mann. Alice Falls into a Black Hole: Entanglement in Noninertial Frames. *Physical Review Letters*, 95:120404, 2005.

[25] S. A. Fulling. Nonuniqueness of canonical field quantization in Riemannian space-time. *Physical Review D*, 7(10):2850–2862, 1973.

[26] R. Gilmore. *Lie groups, physics, and geometry: an introduction for physicists, engineers and chemists*. Cambridge University Press, 2008.

[27] R. M. Gingrich and C. Adami. Quantum entanglement of moving bodies. *Physical Review Letters*, 89(27):270402, 2002.

[28] P. Hayden, M. Horodecki, A. Winter, and J. Yard. A decoupling approach to the quantum capacity. *Open Systems and Information Dynamics*, 15:7–19, 2008.

[29] P. Hayden, P. W. Shor, and A. Winter. Random quantum codes from Gaussian ensembles and an uncertainty relation. *Open Systems and Information Dynamics*, 15:71–89, 2008.

[30] A. S. Holevo. Entanglement-breaking channels in infinite dimensions. *Problems of Information Transmission*, 44(3):171–184, 2008.

[31] M. Horodecki, S. Lloyd, and A. Winter. Quantum coding theorem from privacy and distinguishability. *Open Systems and Information Dynamics*, 15:47–69, 2008.

[32] R. Jozsa. Fidelity for mixed quantum states. *Journal of Modern Optics*, 41:2315–2323, 1994.

[33] A. Kent. Unconditionally secure bit commitment. *Physical Review Letters*, 83:1447–1450, 1999.

[34] R. Klesse. Approximate quantum error correction, random codes, and quantum channel capacity. *Physical Review A*, 75(6):062315–+, 2007.

[35] D. Kretschmann and R. F. Werner. Tema con variazioni: quantum channel capacity. *New Journal of Physics*, 6:26–+, 2004.

[36] S. Lloyd. Capacity of the noisy quantum channel. *Physical Review A*, 55(3):1613–1622, 1997.

[37] E. Martin-Martinez and J. León. Quantum correlations through event horizons: Fermionic versus bosonic entanglement. *Physical Review A*, 81(3):32320, 2010.

[38] U. M. Maurer et al. The strong secret key rate of discrete random triples. *Kluwer International Series In Engineering And Computer Science*, pages 271–271, 1994.

[39] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 2000.

[40] L. Parker. Particle creation in expanding universes. *Physical Review Letters*, 21(8):562–564, 1968.

[41] A. Peres and D. R. Terno. Quantum information and relativity theory. *Reviews of Modern Physics*, 76:93–123, 2004.

[42] R. Schützhold and W. G. Unruh. Comment on "Teleportation with a uniformly accelerated partner". *arXiv:quant-ph/0506028*.

[43] P. W. Shor. The quantum channel capacity and coherent information. Lecture notes, MSRI workshop on quantum computation,http://www.msri.org/publications/ln/msri/2002/quantumcrypto/shor/1/, November 2002.

[44] A. Uhlmann. The 'transition probability' in the state space of a $*$-algebra. *Reports on Mathematical Physics*, 9:273, 1976.

[45] W. G. Unruh. Notes on black-hole evaporation. *Physical Review D*, 14(4):870–892, 1976.

[46] W. G. Unruh and R. M. Wald. What happens when an accelerating observer detects a Rindler particle. *Physical Review D*, 29(6):1047–1056, 1984.

[47] R. M. Wald. *Quantum field theory in curved spacetime and black hole thermodynamics*. University of Chicago Press, Chicago, 1999.