Quantum entanglement theory in the presence of superselection rules

Norbert Schuch, Frank Verstraete, and J. Ignacio Cirac

Max-Planck-Institut für Quantenoptik, Hans-Kopfermann-Str. 1, D–85748 Garching, Germany.

Superselection rules severely constrain the operations which can be implemented on a distributed quantum system. While the restriction to local operations and classical communication gives rise to entanglement as a nonlocal resource, particle number conservation additionally confines the possible operations and should give rise to a new resource. In [Phys. Rev. Lett. **92**, 087904 (2004), quant-ph/0310124] we showed that this resource can be quantified by a single additional number, the superselection induced variance (SiV) without changing the concept of entanglement. In this paper, we give the results on pure states in greater detail; additionally, we provide a discussion of mixed state nonlocality with superselection rules where we consider both formation and distillation. Finally, we demonstrate that SiV is indeed a resource, i.e., that it captures how well a state can be used to overcome the restrictions imposed by the superselection rule.

I. INTRODUCTION

One of the most interesting results in quantum information theory has been the discovery that the amount of nonlocality contained in a bipartite quantum system can be quantified by a single number, the entropy of entanglement (EoE). Asymptotically, multiple copies of any two states can be converted into each other and thus into singlets provided that the total EoE is conserved [1]. On the other hand, entanglement is the key resource for some of the most interesting tasks in quantum information, as teleportation [2] and dense coding [3].

Entanglement has its origin in the restriction to those transformations which can be implemented by local operations and classical communication (LOCC) [4, 5]. In the same way, any additional restriction should lead to another nonlocal quantity and thus to new effects and applications. It has been noted by Popescu [6] that in many physical systems of interest such a restriction is given by a superselection rule (SSR). In this work, we will consider particle number conservation as a superselection rule; this is motivated, e.g., by recent quantum optical experiments on cold atomic gases. Indeed, the notion of entanglement is affected by the additional restrictions [7, 8], and new protocols arise, e.g., perfect data hiding [9] becomes possible [7]. On the other hand, it has been shown [7, 10] that the extra resource of a shared reference frame (i.e., a nonlocal state) allows to overcome the restrictions imposed by the SSR (note that [10] also adressed non-Abelian SSR); conversely, private reference frames restrict the possible operations of an eavesdropper and can thus be employed for cryptographic tasks [11].

In [12], we have shown that the nonlocality contained in a bipartite state subject to SSR can be quantified by only one additional number, the *superselection induced variance* (SiV): any two states can be interconverted asymptotically as long as the total EoE *and* SiV are conserved. In this paper, we prove this result in greater detail and extend it to mixed states. We start by discussing how the majorization criterion [13] which governs the conversion of quantum states has to be changed

when SSR are present, and show that it asymptotically converges to the conservation of EoE (as it is the case without SSR) and SiV. We give a detailed proof of this result for arbitrary states and show that it motivates the definition of two different types of standard forms for SiV which carry a linear resp. logarithmic amount of EoE.

While there exist pure states which carry only EoE, there are no pure states which contain solely SiV. On the other hand, it has been demonstrated [7] that there exist separable but nonlocal mixed states, i.e., states which have a separable decomposition and thus do not contain EoE, but are still nonlocal as all these decompositions violate the SSR and therefore should contain SiV. In order to make these statements quantitative, we extend the concepts of EoE and SiV to mixed states subject to SSR. One natural way to do this is to consider the amount of pure states resources needed to create the state [14]; we show that this extension can be done in a meaningful way and that there indeed exist states which contain SiV but no EoE. The converse way is to ask whether it is possible to distill pure state resources from some mixed state [15]; we provide ways to distill both EoE and SiV, and we show that it is even possible to distill the SiV contained in separable states.

EoE is a *resource*—it allows to overcome the LOCC restrictions by teleportation. It is reasonable to assume that any restriction leads to a nonlocal quantity which in turn allows to overcome this restriction. Indeed, we give evidence that SiV can be used as a resource which allows to overcome the additional restrictions imposed by the SSR in a bipartite setting (cf. [7, 12]). Therefore, we will use two tasks: distinguishing locally undistinguishable quantum states and teleporting states with nonconstant local particle number [7]. We will show that not only pure states can be used as share reference frames for these tasks, but that there even exist separable states which together with one ebit of entanglement allow to perfectly teleport one qubit and thus to overcome all restrictions. Still, we find that there is a fundamental difference between EoE and SiV as a resource, as a finite amount of nonlocality does not allow to perfectly overcome the re-

strictions which is due to the structure of the underlying Hilbert space [12].

The paper is organized as follows. In Sec. II, we introduce the concept of a superselection rule and show how it restricts the operations which can be implemented in a bipartite setting. In Sec. III, we consider the conversion of pure states. We start with the conversion of single copies, which motivates the definition of SiV as a nonlocal monotone; then, we prove that asymptotically all states can be converted given that both SiV and EoE are conserved. Sec. IV is devoted to mixed state nonlocality. First, we discuss formation of mixed states; beyond other results, we provide explicit formulas for the case of qubits. Second, we give different methods for the distillation of both EoE and SiV independently as well as simultaneously. Finally, Sec. V discusses SiV as a resource; there, we quantify how well states with SiV can be used as shared reference frames which allow to overcome the new restrictions, and we demonstrate that one ebit of entanglement is still sufficient for teleportation.

II.   PARTICLE NUMBER CONSERVATION AS A SUPERSELECTION RULE

In this paper, we focus on particle number conservation as a SSR, but the results also apply to charge and other discrete quantities. In this case, the Hilbert space of the system $\mathcal{H}$ can be decomposed into a direct sum $\mathcal{H} = \bigoplus_{N=0}^{\infty} \mathcal{H}_N$ of the eigenspaces of the particle number operator $\hat{N}$, and the SSR imposes that for any operator $\mathcal{O}$, $[\mathcal{O}, \hat{N}] = 0$ must hold; thus, any operator can be written as a sum of operators $\mathcal{O}_N$ which have support on $\mathcal{H}_N$ only, $\mathcal{O} = \bigoplus_{N=0}^{\infty} \mathcal{O}_N$, and thus

$$\mathcal{O} = \sum_N P_N \mathcal{O} P_N , \qquad (1)$$

where P_N projects onto $\mathcal{H}_N$. As the same restriction holds for the admissible density operators, all states can be converted into each other, and no interesting new effects can be found.

Therefore, we consider SSR in a bipartite setting. Then, we have local particle number operators $\hat{N}_A$ and $\hat{N}_B$, and the total particle number operator is given by

$$\hat{N}_{AB} = \hat{N}_A \otimes \mathbb{1}_B + \mathbb{1}_A \otimes \hat{N}_B . \qquad (2)$$

While the admissible states have to commute with the global particle number operator $\hat{N}_{AB}$, the local operations have to commute with the local particle number operators $\hat{N}_A$ and $\hat{N}_B$. This restriction is stronger than the one given by the bipartite setting alone and should therefore lead to a new nonlocal resource. More precisely, the operations on subspaces with fixed total particle number $N = N_{AB}$ are given by

$$\mathcal{O}_N^{AB} = \bigoplus_{N_A + N_B = N} \left(\mathcal{O}_{N_A}^A \otimes \mathbb{1}_{N_B}^B \right) \qquad (3)$$

(and vice versa)—in addition to the restriction to products $\mathcal{O}^A \otimes \mathbb{1}$ imposed by the bipartite setting, a direct sum structure arises from the SSR. This product vs. sum structure will reappear throughout the paper and is the reason for some fundamental differences between EoE (arising for the product structure) and SiV (arising from the direct sum).

The restriction to block-diagonal operations, Eq. (1), can be relaxed by adding ancilla modes with m_0 particles, performing a block-diagonal unitary U, and measuring resp. tracing out the ancillas. Then, the admissible (POVM/Kraus) operators are given by $\mathcal{O} = P_m^{\mathrm{anc}} U P_{m_0}^{\mathrm{anc}}$; by applying (1) to U, this leads to $\mathcal{O} = \sum_N P_{N+\Delta} \mathcal{O} P_N$ (resp. $[\hat{N}, \mathcal{O}] = \Delta \mathcal{O}$, Δ might differ for each $\mathcal{O}$): $\mathcal{O}$ can shift the particle number by some Δ. (Note that $\mathcal{O}^\dagger \mathcal{O}$ remains block-diagonal). As most results of this paper are only affected marginally by including ancillas, we will usually neglect them and just briefly comment on their effect as appropriate.

At the end of this section, let us introduce a few notational conventions. Logarithms are taken to the basis 2. A ket $|N\rangle$ denotes a state with N particles. We will use this notation even if the underlying eigenspace is degenerate, unless the nonlocal properties under consideration depend on this degeneracy.

The restrictions imposed by the SSR on the allowed operations can be easily overcome by defining a new computational basis $|\hat{0}\rangle \equiv |01\rangle$, $|\hat{1}\rangle \equiv |10\rangle$ in which all states have the same particle number [7]. This motivates the definition of two different types of maximally entangled two-qubit states,

$$|\text{V-EPR}\rangle = |0\rangle_A |1\rangle_B + |1\rangle_A |0\rangle_B$$

(a "variance-EPR", as there is some variance in the local particle number), and

$$|\text{E-EPR}\rangle = |01\rangle_A |10\rangle_B + |10\rangle_A |01\rangle_B \equiv |\hat{0}\rangle_A |\hat{1}\rangle_B + |\hat{1}\rangle_A |\hat{0}\rangle_B$$

(an "entanglement-EPR", which is defined within an unrestricted subspace and only carries entanglement). The very difference between these two states will be a central issue of the paper.

III.   CHARACTERIZATION OF PURE STATES

In this section, we characterize pure states in a bipartite setting, i.e., we determine the possible conversions by LOCC and thus quantify the nonlocality contained in a bipartite state. Without superselection rules, the majorization criterion determines whether the conversion between two bipartite pure states is possible [13, 16]. The conversion of multiple copies is governed by a much simpler criterion: it has been shown [1] that multiple copies of any two states can be interconverted reversibly. The conversion ratio is determined by only one quantity which fully characterizes the nonlocal properties of a bipartite state, the *entropy of entanglement* (EoE).

As we have seen in the preceding section, in addition to the tensor product structure induced by the bipartite setting the operators have to obey a direct sum structure. In this section, we show that these two structures lead to two complementary resources: while the tensor product again induces the majorization criterion and (asymptotically) EoE as a nonlocal resource, the direct sum gives rise to additional restrictions on the conversions of states and in turn leads to an own nonlocal resource.

A. The single copy case

Let us consider the following problem: given pure bipartite states ϕ and ψ, is it possible to convert ϕ to ψ by LOCC? This task can be generalized naturally to a set of outcomes $\{(p_i, \psi_i)\}$, where each outcome ψ_i is obtained with probability p_i.

Let us first see how this can be solved without SSR [13]. Therefore, let $\boldsymbol{\lambda} = (\lambda_k)$ and $\boldsymbol{\mu}^i = (\mu_k^i)$ be the Schmidt coefficients of ϕ and ψ_i, respectively, which completely characterize the states up to local unitaries. Without loss of generality, the Schmidt vectors may be taken decreasing ($\lambda_k \geq \lambda_{k+1}$) and of equal dimension (by appending zeros). Following [13], an LOCC strategy for the conversion

$$\phi \longrightarrow \{(p_i, \psi_i)\}$$

exists if and only if (iff)

$$\boldsymbol{\lambda} \prec \sum_i p_i \boldsymbol{\mu}^i .$$

Here, for two ordered vectors $\boldsymbol{\lambda}$ and $\boldsymbol{\mu}$, we say that $\boldsymbol{\lambda}$ *is majorized by* $\boldsymbol{\mu}$, $\boldsymbol{\lambda} \prec \boldsymbol{\mu}$, if $\sum_{k=1}^d \lambda_k \leq \sum_{k=1}^d \mu_k$ for all $1 \leq d < \dim \boldsymbol{\lambda}$, where equality holds for $d = \dim \boldsymbol{\lambda}$.

As an example, consider the states

$$|\phi\rangle = \sqrt{\tfrac{1}{2}}|0\rangle_A|1\rangle_B + \sqrt{\tfrac{1}{2}}|1\rangle_A|0\rangle_B \text{ and}$$

$$|\psi\rangle = \sqrt{\tfrac{1}{3}}|0\rangle_A|1\rangle_B + \sqrt{\tfrac{2}{3}}|1\rangle_A|0\rangle_B ,$$

which have the ordered Schmidt vectors $\boldsymbol{\lambda} = (1/2, 1/2)$ and $\boldsymbol{\mu} = (2/3, 1/3)$, respectively. Since $\boldsymbol{\lambda} \prec \boldsymbol{\mu}$, it is possible to convert $\phi \to \psi$; for instance, Alice might start with the POVM measurement given by $M_1 = \sqrt{1/3}|0\rangle\langle 0| + \sqrt{2/3}|1\rangle\langle 1|$ and $M_2 = \sqrt{1/3}|0\rangle\langle 0| + \sqrt{2/3}|1\rangle\langle 1|$ which yields the two states

$$|\psi_1\rangle = \sqrt{\tfrac{1}{3}}|0\rangle_A|1\rangle_B + \sqrt{\tfrac{2}{3}}|1\rangle_A|0\rangle_B \text{ and}$$

$$|\psi_2\rangle = \sqrt{\tfrac{2}{3}}|0\rangle_A|1\rangle_B + \sqrt{\tfrac{1}{3}}|1\rangle_A|0\rangle_B .$$

with equal probabilities: ψ_1 is already equal to ψ, and ψ_2 can be converted to ψ by a bilateral NOT operation.

Let us now see what is different when SSR apply: while the POVM measurement $\{M_1, M_2\}$ is compatible with the superselection rule, the local application of NOT operations is not; indeed, it is not possible at all to carry out $\phi \to \psi$ deterministically in the presence of SSR. In order to see this, define block-diagonal POVM operators $M_i = \bigoplus_n M_n^i$ on one local system. Then, the completeness relation $\sum M_i^\dagger M_i = \mathbb{1}$ yields $\sum_i M_n^{i\dagger} M_n^i = \mathbb{1}$ for all n. Therefore, any POVM operator is simply a direct sum of POVM operators acting within the subspaces with constant local particle number, i.e., the usual conditions for convertibility have to hold for each subspace separately. Particularly, this implies that for pure states the *average weight* of each subspace with constant local particle number *cannot be changed* by local operations.

The impossibility to change the average weight of a subspace with fixed local particle number can even be proven at a much more fundamental level. Take multiple copies of some state $|\phi\rangle$ with nonconstant local particle number, and assume there is a way for Alice to change her local particle number distribution on average. As the total particle number is constant, this implies that the average particle number distribution of Bob's system is changed the other way round. Therewith, Alice can change Bob's density matrix remotely which would allow for supraluminal communication and therefore has to be ruled out. Classical communication between Alice and Bob, on the other hand, will increase Bob's knowledge of the *actual* particle number distribution, but it cannot influence the *average* distribution obtained.

In order to formulate this result precisely, note that any bipartite state $\phi \in \mathcal{H}_N$ subject to SSR can be written as $\phi = \phi^0 \oplus \cdots \oplus \phi^N$ with $\phi^n \in \mathcal{H}_n^A \otimes \mathcal{H}_{N-n}^B$, i.e., as a direct sum of unnormalized pure states with constant local particle number. Call the (ordered) *unnormalized* Schmidt coefficients of ϕ^n $\boldsymbol{\lambda}^n$. Then, ϕ is characterized up to local (SSR-compatible) unitaries by its *SSR-ordered Schmidt vector* $\boldsymbol{\lambda} = (\boldsymbol{\lambda}^0, \ldots, \boldsymbol{\lambda}^N)$.

Theorem 1 ([17]). *Let ϕ, ψ_i be pure states and $\boldsymbol{\lambda}$, $\boldsymbol{\mu}_i$ their SSR-ordered Schmidt vectors. Then,*

$$\phi \xrightarrow{\text{SSR}} \{(p_i, \psi_i)\} \tag{4}$$

(i.e., there exists a SSR-compatible conversion strategy) if and only if

$$\boldsymbol{\lambda}^n \prec \sum_i p_i \boldsymbol{\mu}_i^n \quad \forall n = 0, \ldots, N. \tag{5}$$

In order to see the connection to the conversions within the subspaces, let us re-express (5) by normalizing the SSR-ordered Schmidt vectors,

$$\hat{\boldsymbol{\lambda}}^n \prec \sum_i \underbrace{p_i \frac{\|\boldsymbol{\mu}_i\|}{\|\boldsymbol{\lambda}\|}}_{=:p_i'} \hat{\boldsymbol{\mu}}_i^n \quad \forall n = 0, \ldots, N ,$$

where in the following a hat $\hat{\cdot}$ denotes the normalized vector. According to the usual majorization result, this holds iff we can convert

$$\hat{\phi}^n \longrightarrow \{p_i', \hat{\psi}_i^n\} \quad \forall n = 0, \ldots, N . \tag{6}$$

Here, $\phi = \phi^0 \oplus \cdots \oplus \phi^N$ and $\psi_i = \psi_i^0 \oplus \cdots \oplus \psi_i^N$.

Proof. Exactly as without SSR, the most general strategy consists of Alice performing a generalized measurement and communicating the result to Bob, who then applies a unitary operation depending on the measurement outcome; the proof [18] can be directly transferred.

We show (4)$\Leftrightarrow$(6). The proof can be restricted to the case where each conversion $\phi \to (p, \psi)$ in (4) resp. (6) can be accomplished by a single POVM operator M, i.e., $M\phi = \sqrt{p}\psi$—otherwise, we can split $\phi \to (p, \psi)$ into $\phi \to (p_k, \psi)$, $\sum p_k = p$, where each conversion is the result of *one* of the POVM operators. This can be done as well for the system of conversions (6), where we have to split all subspaces simultaneously (this can be always done by additionally splitting single POVM operators into copies of itself).

First, assume that (4) holds. Then there exist POVM operators $M_i = \bigoplus_n M_i^n$ on Alices side for which $M_i\phi \cong_B \sqrt{p_i}\psi$ (i.e., up to a unitary on Bob's side). Decomposing this into the subspaces in the direct sum, one obtains $M_i^n\phi^n \cong_B \sqrt{p_i}\psi_i^n$ and thus

$$M_i^n\hat{\phi}^n \cong_B \underbrace{\sqrt{p_i \frac{\langle \psi_i | \psi_i \rangle}{\langle \phi | \phi \rangle}}}_{\equiv \sqrt{p_i'}} \hat{\psi}_i^n$$

for all N, i.e., the M_i^n accomplish the set of conversions given by Eq. (6). Especially, as

$$\mathbb{1} = \sum_i \left(\bigoplus_n M_i^n \right)^\dagger \left(\bigoplus_n M_i^n \right) = \bigoplus_n \left(\sum_i M_i^{n\dagger} M_i^n \right) ,$$

the M_i^n obey the completeness relation for POVM operators. As all arguments hold in both directions, this completes the proof. □

B. Variance as a nonlocal monotone

Let us now formulate an asymptotic version of the previous theorem. It is known that without SSR for a large number of copies the majorization criterion converges to the entropic criterion, i.e., the conservation of the total EoE [1]. With SSR, the probability distribution associated to the variation of the local particle number, $p_n = \sum_i p_i^n$, has to be conserved as well. Asymptotically, this distribution converges to a Gaussian which is completely characterized by its mean (which can be shifted using ancillas) and its variance. Therefore we define

Definition 1. *For a bipartite pure state ϕ shared by A and B, define the superselection induced variance (SiV)*

$$V(\phi) := 4 \left[\langle \phi | \hat{N}_A^2 | \phi \rangle - \langle \phi | \hat{N}_A | \phi \rangle^2 \right] ,$$

where N_A is the particle number operator for Alice. (One could equally well take $\hat{N}_B$, as $\hat{N}_A + \hat{N}_B = N = \text{const.}$)

The factor 4 in the definition normalizes the SiV: $V(|\text{V-EPR}\rangle) = 1$.

Let us now show that SiV is really an entanglement monotone [19] when SSR are present, namely that it cannot be increased on average by SSR-LOCC and vanishes on separable states. (On the contrary, note that $V(\phi) = 0$ does *not* imply that ϕ is separable—this is due to the fact that there exist two different nonlocal quantities when SSR are present.) Moreover, SiV is symmetric under interchange of A and B and additive: given two subsystems 1 and 2 shared by A and B, $V(\phi_1 \otimes \phi_2) = V(\phi_1) + V(\phi_2)$, as can be readily seen by applying Eq. (2) to the two subsystems 1 and 2, $\hat{N}_{A1\,A2} = \hat{N}_{A1} \otimes \mathbb{1}_{A2} + \mathbb{1}_{A1} \otimes \hat{N}_{A2}$.

To show the monotonicity of SiV under SSR-LOCC, consider a POVM measurement $\{M_i^A\}$ on Alice's side. Then, the average SiV after the application of $\{M_i^A\}$ is given by

$$\bar{V}_M(\phi) = \sum_i \langle \phi | M_i^{A\dagger} \hat{N}_A^2 M_i^A | \phi \rangle - \sum_i \frac{\langle \phi | M_i^{A\dagger} \hat{N}_A M_i^A | \phi \rangle^2}{\langle \phi | M_i^{A\dagger} M_i^A | \phi \rangle} .$$

The first part reduces to $\langle \phi | \hat{N}_A^2 | \phi \rangle$ (using $[\hat{N}_A, M_i^A] = 0$ and $\sum_i M_i^{A\dagger} M_i^A = \mathbb{1}$), while for the second part

$$\sum_i \frac{\langle \phi | M_i^{A\dagger} \hat{N}_A M_i^A | \phi \rangle^2}{\langle \phi | M_i^{A\dagger} M_i^A | \phi \rangle} \overset{(*)}{\geq} \left(\sum_i \langle \phi | M_i^{A\dagger} \hat{N}_A M_i^A | \phi \rangle \right)^2$$
$$= \langle \phi | \hat{N}_A | \phi \rangle^2 .$$

Here, $(*)$ has been derived using the Cauchy-Schwarz inequality

$$\left(\sum_i y_i \right)^2 = \left(\sum_i \sqrt{p_i} \frac{y_i}{\sqrt{p_i}} \right)^2 \leq \sum_i \frac{y_i^2}{p_i} \sum_{i'} p_{i'} . \quad (7)$$

Ancillas leave the result unaffected, as the extra contributions in $\bar{V}_M(\phi)$ originating from $[\hat{N}, \mathcal{O}] = \nu\mathcal{O}$ cancel out.

C. Reversible conversion of multiple copies

The introduction of SiV as a nonlocal monotone was motivated by the conversion of multiple copies, as it characterizes the joint particle number distribution. In the following, we will show that asymptotically SiV and EoE quantify the two complementary resources which completely characterize bipartite states up to SSR-LOCC.

Theorem 2. *In the presence of SSR, there exists an asymptotically reversible conversion*

$$|\phi\rangle^{\otimes N} \otimes |\hat{0}\rangle^{\otimes E(\phi)N} \longleftrightarrow \sum_n c_n |n\rangle |N-n\rangle \otimes |\text{E-EPR}\rangle^{\otimes E(\phi)N},$$

where the coefficients c_n are distributed Gaussian with SiV $N V(|\phi\rangle)$.

Note that on the left hand side we have added ancilla states in the unrestricted "hat"–basis (cf. Sec. II). The conversion transfers the entanglement contained in $|\phi\rangle^{\otimes N}$ to this second register as "accessible" entanglement in the form of $|$E-EPR$\rangle$s, while the SiV stays in the first register.

Proof. First, we restrict ourself to the case of qubits, where $|\phi\rangle = \sqrt{p_0}|0\rangle|1\rangle + \sqrt{p_1}|1\rangle|0\rangle$. We will generalize the result in two steps: in a first step, we consider qu-d-its, where the local basis is $\{|0\rangle, \ldots, |d-1\rangle\}$, while in a second step we allow for arbitrary bipartite states, i.e., the local bases might contain several states with the same particle number.

For the beginning, let us only look at the first register. Taking N copies of $|\phi\rangle$, we have

$$|\phi\rangle^{\otimes N} = \sum_{\mathbf{x}} \sqrt{p_0^{n_0} p_1^{n_1}} |\mathbf{x}\rangle|\neg\mathbf{x}\rangle ,$$

where the sum is taken over all possible N-bit strings $\mathbf{x}$. Here, n_0 and n_1 are the numbers of zeroes and ones in $\mathbf{x}$, respectively, and $\neg\mathbf{x}$ denotes the bitwise NOT of $\mathbf{x}$. This state can be grouped naturally as

$$|\phi\rangle^{\otimes N} = \sum_{n_0} \sqrt{p_0^{n_0} p_1^{N-n_0} \binom{N}{n_0}} |\chi_{N-n_0,n_0}\rangle , \quad (8)$$

where the state $|\chi_{N-n_0,n_0}\rangle \in \mathcal{H}_{N-n_0}^A \otimes \mathcal{H}_{n_0}^B$ is a maximally entangled state with Schmidt number $\binom{N}{n_0}$.

In the following, we show how to transfer the entanglement of $|\phi\rangle^{\otimes N}$ to the second register. Therefore, we have to break the tensor product structure $|\phi\rangle^{\otimes N}$ of the first register and create a new tensor product structure by properly transferring the entanglement to the second register. To this end, let us introduce the concept of typical subspaces [20]. An ϵ-typical subspace of our Hilbert space is defined as $\mathcal{H}_\epsilon = \bigoplus_{n_0 \in \mathcal{S}_\epsilon} \mathcal{H}_{N-n_0}^A \otimes \mathcal{H}_{n_0}^B$, where the ϵ-typical n_0 are those lying in $\mathcal{S}_\epsilon = \{n_0 : |n_0/N - p_0| < \epsilon\}$. It can be shown [20, 21] that projecting $|\phi\rangle^{\otimes N}$ onto $\mathcal{H}_\epsilon$ gives an error which vanishes for $N \to \infty$ such that we can restrict the sum in (8) to $n_0 \in \mathcal{S}_\epsilon$. Then,

$$\binom{N}{n_0} \geq \frac{1}{(N+1)^2} 2^{NH(\frac{n_0}{N})} \geq 2^{N[H(p_0)-K\epsilon]} \quad (9)$$

with some $K > 0$ holds for all $n_0 \in \mathcal{S}_\epsilon$ ($\epsilon \ll 1$ and $N \gg 1$) [20]; here $H(p) = H(p, 1-p)$ is the Shannon entropy of the probability distribution $(p, 1-p)$. According to Theorem 1, we can transform

$$|\chi_{N-n_0,n_0}\rangle \to \frac{1}{\sqrt{E}} \sum_{i=1}^{E} |i_{N-n_0}\rangle_A |i'_{n_0}\rangle_B ; \ E = H(p_0) - K\epsilon$$

coherently in all subspaces in the restricted sum, where $|i_n\rangle$ are orthogonal states with n particles. Then by local maps $|i_n\rangle|\hat{0}\rangle \mapsto |n\rangle|\hat{i}\rangle$, where $|\hat{i}\rangle$ are orthogonal and

$|n\rangle = |1\cdots10\cdots0\rangle$, the entanglement $H(p_0) - K\epsilon$ can be transferred to the second register which gives

$$\sum_{n_0 \in \mathcal{S}_\epsilon} c_{n_0} |N-n_0\rangle|n_0\rangle \otimes \Big[|01\rangle|10\rangle + |10\rangle|01\rangle\Big]^{\otimes N[H(p_0)-K\epsilon]},$$
(10)

where $c_{n_0} = \sqrt{p_0^{n_0} p_1^{N-n_0} \binom{N}{n_0}}$. The sum can be extended to all n_0 with high fidelity, and the $|c_{n_0}|^2$ approach a Gaussian distribution with variance $Np_0(1-p_0) = V(\phi)/4$. This is the only parameter characterizing the state (10), since the mean can be shifted by locally adding ancillas. As $H(p_0)$ is just $E(\phi)$, this completes the distillation direction of the proof.

The dilution direction can be proven using the converse of (9),

$$\binom{N}{n_0} \leq 2^{NH(\frac{n_0}{N})} \leq 2^{N[H(p_0)+K\epsilon]} ,$$

in an ϵ-typical subspace. Starting from

$$\sum_{n_0 \in \mathcal{S}_\epsilon} c_{n_0} |N-n_0\rangle|n_0\rangle \otimes \Big[|01\rangle|10\rangle + |10\rangle|01\rangle\Big]^{\otimes N[H(p_0)+K\epsilon]},$$

we can transfer the entanglement to the first register and then (again by Theorem 1) reduce the Schmidt number of each subspace to $\binom{N}{n_0}$, obtaining the projection of $|\phi\rangle^{\otimes N}$ onto the ϵ-typical subspace, so that the dilution works as well. This completes the proof for qubits.

In a first step, we generalize the proof from qubits to $(I+1)$-level systems,

$$|\phi\rangle = \sum_{i=0}^{I} \sqrt{p_i} |i\rangle|I-i\rangle . \quad (11)$$

(Note that the coefficients can be made positive by local operations.) Again, for N copies of $|\phi\rangle$, an ϵ-typical subspace can be defined by restricting the number n_i of occurences of the state $|i\rangle|I-i\rangle$ in the product by $|n_i/N - p_i| < \epsilon$ for all i. Projecting the state onto an ϵ-typical subspace again only yields a vanishingly small error, and the Schmidt number of the states with fixed numbers $(n_0, \ldots, n_I)$ is given by the multinomial coefficient $\binom{N}{n_0 \cdots n_I}$ and obeys the bounds [20]

$$2^{N[E(\phi)-K\epsilon]} \leq \binom{N}{n_0 \ \cdots \ n_I} \leq 2^{N[E(\phi)+K\epsilon]} .$$

Thus, it is possible to extract the entanglement $E(\phi)$ reversibly. Yet, there are several possible configurations $(n_0, \ldots, n_I)$ which yield the same local particle number $n = \sum_i i n_i$ such that there is still some entanglement left in each subspace. But as for N copies of $|\phi\rangle$ the number of these configurations is bounded by N^I, this entanglement is logarithmic in N and can be removed reversibly.
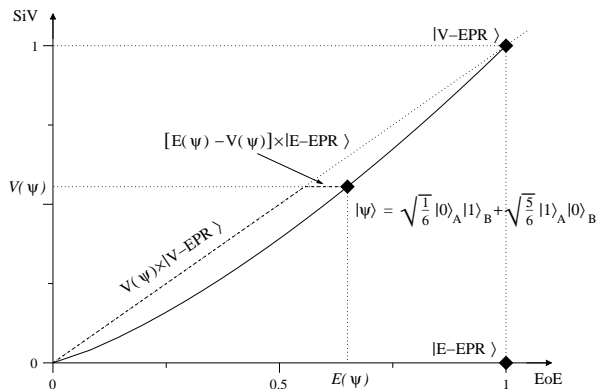
FIG. 1: Characterization of pure qubit states in an E-V diagram. All the states reside on the solid curve; asymptotically, any state can be converted into $V(\psi)$ copies of a $|\text{V-EPR}\rangle$ and $E(\psi) - V(\psi)$ of a $|\text{E-EPR}\rangle$.

Therefore, we can reversibly transform $|\phi\rangle^{\otimes N} \otimes |\hat{0}\rangle^{\otimes NE(\phi)}$ into

$$\sum c_n |n\rangle |IN - n\rangle \otimes \Big[|01\rangle|10\rangle + |10\rangle|01\rangle \Big]^{\otimes NE(\phi)} , \quad (12)$$

where the c_n are given by the sum over all coefficients for which the particle number on Alice's side is n,

$$c_n = \sqrt{ \sum_{\substack{\sum_i i n_i = n \\ \sum_i n_i = N}} p_0^{n_0} \cdots p_I^{n_I} \begin{pmatrix} N \\ n_0 \ \cdots \ n_I \end{pmatrix} } \quad .$$

It remains to be shown that the $|c_n|^2$ approach a Gaussian distribution. As long as all $p_i \neq 0$, this can be shown by expanding each n_i within the typical subspace as $n_i = N(p_i + \delta_i)$ with $\delta_i < \epsilon$. This will work fine whenever $Np_i \gg 1$ and $\epsilon \ll p_i$ for all i. Yet, this condition cannot be satisfied if $p_i = 0$ for some i. This might (but need not!) lead to a periodic gap in the distribution of the $|c_n|^2$, e.g., for $I = 2$, $p_0 = p_2 = 1/2$. In that case, $|c_n|^2 = 0$ for all odd n.

In principle, such a gap has to be considered as a third nonlocal characteristic of a bipartite state. Still, it can be removed easily. In the example given above the gap is readily removed by adding *one* $|\text{V-EPR}\rangle$, such that the fraction of $|\text{V-EPR}\rangle$ per copies of $|\phi\rangle$ vanishes. By further adding an $|\text{E-EPR}\rangle$ (those are obtained anyway in the distillation) the $|\text{V-EPR}\rangle$ can be re-obtained—it therefore merely acts as a catalyst, "freeing" the subspaces with odd particle number.

The generalization to an arbitrary state is straightforward. Take

$$|\phi\rangle = \sum_{i=0}^{I} \sqrt{p_i} |\psi_{i,I-i}\rangle , \quad (13)$$

where $|\psi_{i,I-i}\rangle \in \mathcal{H}_i^A \otimes \mathcal{H}_{I-i}^B$ might themselves be entangled states. Applying the concept of typical subspaces to Eq. (13), we find that the number of occurences of each
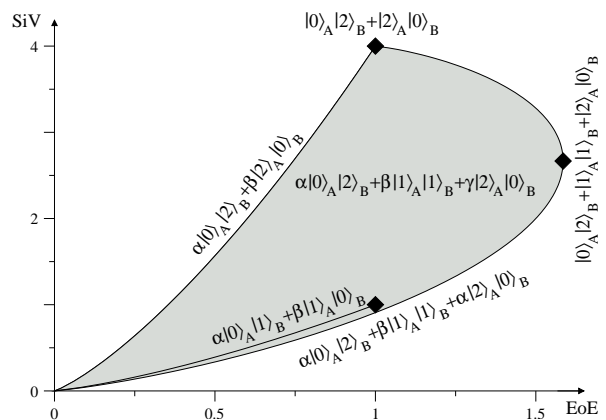

FIG. 2: E-V diagram for qutrits, where the boundary states and the extremal states are given. The possible states reside in the gray area, the solid line within this area is the subset realizable by qubits.

$|\psi_{i,I-i}\rangle$ in the typical subspace is bounded by $(p_i \pm \epsilon)N$, and thus the entanglement $E(\psi_{i,I-i})$ contained in these states—which is already "accessible entanglement"—can be extracted reversibly. The remaining state is of the type of Eq. (11) (with the same coefficients p_i) and thus can be transformed reversibly into a Gaussian distributed state with width $NV(\phi)$ and $NH(p_0, \ldots, p_I)$ ebits of entanglement. It can be checked easily that the total number of Bell pairs is $NE(\phi)$. $\quad\square$

For qubits, Theorem 2 can be re-expressed.

Corollary 1. *For bipartite qubit states $|\phi\rangle$,*

$$|\phi\rangle \longleftrightarrow |\text{E-EPR}\rangle^{\otimes[E(\phi)-V(\phi)]} |\text{V-EPR}\rangle^{\otimes V(\phi)}$$

in the asymptotic limit.

This can be shown by applying Theorem 2 twice, together with $E(\phi) \geq V(\phi)$ (which only holds for qubits).

Fig. 1 illustrates this characterization of states in the E-V diagram. Fig. 2 shows the E-V diagram for qutrits, which is considerable more complex. The bounds are given by the states with highest variance $\alpha|0\rangle_A|2\rangle_B + \beta|2\rangle_A|0\rangle_B$ and the states with highest entanglement $\alpha|0\rangle_A|2\rangle_B + \beta|1\rangle_A|1\rangle_A + \alpha|0\rangle_A|2\rangle_B$. A decomposition as in the Corollary is still possible if one replaces the $|\text{V-EPR}\rangle$ by $|0\rangle_A|2\rangle_B + |2\rangle_A|0\rangle_B$ which has maximal variance.

IV. MIXED STATES IN THE PRESENCE OF SUPERSELECTION RULES

A. Introduction

In the following section, we consider mixed states. We will show how the concepts of EoE and SiV as two complementary resources can be extended to mixed states,

and discuss the connection with normal (SSR-free) entanglement measures.

Let us start by introducing a particularly interesting mixed state,

$$\rho_{\text{sep}} = \frac{1}{4} \begin{pmatrix} 1 & & & \\ & 1 & 1 & \\ & 1 & 1 & \\ & & & 1 \end{pmatrix} \qquad (14)$$

in the basis $\{|0\rangle_A|0\rangle_B, |0\rangle_A|1\rangle_B, |1\rangle_A|0\rangle_B, |1\rangle_A|1\rangle_B\}$. This state has first been considered in [7], where it was shown that it is separable but nonlocal. Namely, it can be obtained by mixing $(|0\rangle_A + \omega|1\rangle_A)(|0\rangle_B + \omega|1\rangle_B)$ for $\omega \in \{1, i, -1, -i\}$ with equal probabilities and therefore does not contain EoE. On the other hand, it is easy to see that there is no decomposition of ρ_{sep} which is separable *and* compatible with the superselection rule, i.e., it cannot be created locally. Clearly, this can not happen with pure states.

Considering the results of the preceding section, it is natural to assume that ρ_{sep} contains SiV but no EoE. In order to give quantitative meaning to such statements, we discuss two genuine extensions of nonlocal quantities to mixed states, defined by the asymptotic amount of pure state resources which are needed to create them and which can be extracted again.

B. Formation of mixed states

Let us start with the creation of mixed state in the presence of SSR. Similar to the normal case [14], we define:

Definition 2. *The entanglement of formation and the variance of formation in the presence of superselection rules are defined as*

$$E_F^{\text{SSR}}(\rho) = \min_{\{p_i, \psi_i\}} \sum_i p_i E(\psi_i)$$

and

$$V_F^{\text{SSR}}(\rho) = \min_{\{p_i, \psi_i\}} \sum_i p_i V(\psi_i) ,$$

respectively. The minimum is taken over all possible decompositions of ρ, where the ψ_i have to obey the SSR (i.e., they all have constant particle number).

The entanglement cost [22] and the variance cost in the presence of superselection rules are accordingly defined as the regularized versions of E_F^{SSR} and V_F^{SSR},

$$E_c^{\text{SSR}}(\rho) = \lim_{N \to \infty} \frac{E_F^{\text{SSR}}(\rho^{\otimes N})}{N}$$

and

$$V_c^{\text{SSR}}(\rho) = \lim_{N \to \infty} \frac{E_F^{\text{SSR}}(\rho^{\otimes N})}{N} .$$

These definitions make sense, as they quantify the nonlocal resources we need at least to prepare the state ρ with SSR [22].

As shown at the beginning of the section there exist states which do not contain any entanglement yet are nonlocal, as ρ_{sep} [Eq. (14)]. One easily finds that $E_F^{\text{SSR}}(\rho_{\text{sep}}) = 1/2$, $V_F^{\text{SSR}}(\rho_{\text{sep}}) = 1/2$, as each of the sub-blocks in ρ_{sep} has to be created separately. On the other hand, it seems reasonable to assume that ρ_{sep} can be prepared asymptotically without using entanglement. In the following, we prove an even stronger result: asymptotically, the entanglement needed to create any state ρ is just the entanglement needed without SSR.

Theorem 3. *For any ρ with bounded maximal particle number,*

$$E_c^{\text{SSR}}(\rho) = E_c(\rho) ,$$

i.e., the entanglement cost with SSR is the entanglement cost without SSR.

Proof. Consider a mixed state σ compatible with the SSR and let $\sum_i p_i|\psi_i\rangle\langle\psi_i| = \sigma$ be the optimal decomposition without SSR, i.e., $E_F(\rho) = \sum_i p_i E(\psi_i)$. Clearly, this decomposition need not obey the SSR, but we can use it to constuct a compatible decomposition with vanishing overhead. From (1), $\sigma = \sum_{n=0}^N P_n \sigma P_n$, where P_n is the projector onto the subspace with *totally* n particles and N the maximum total particle number in σ; therefore,

$$\sigma = \sum_{n,i} p_i p_{i,n} \frac{P_n|\psi_i\rangle\langle\psi_i|P_n}{p_{i,n}}$$

with $p_{i,n} = \langle\psi_i|P_n|\psi_i\rangle$ is a decomposition of σ which is compatible with the SSR. For any $|\psi\rangle$ with at most N particles, it holds that the measurement of the total particle number creates at most $\log(N+1)$ entanglement on average,

$$\sum_n \langle\psi|P_n|\psi\rangle E\left(\frac{P_n|\psi\rangle}{\sqrt{\langle\psi|P_n|\psi\rangle}}\right) \leq E(|\psi\rangle) + \log(N+1)$$

$$(15)$$

(the proof is given in the appendix), and with $\sigma = \rho^{\otimes M}$, the claim follows. $\qquad\square$

Note that this also implies that E_F^{SSR} is not additive [8]; $E_F^{\text{SSR}}(\rho_{\text{sep}}^{\otimes N})$, e.g., grows at most logarithmically.

Let us now consider V_F^{SSR} and V_c^{SSR}. As expected, the entanglement cost of ρ_{sep} vanishes. But as ρ_{sep} still contains some kind of nonlocality, it is natural to assume that its variance cost is strictly nonzero. In the following, we prove a more general result, namely that V_F^{SSR} is additive on all states which are a direct sum of pure states (i.e., ρ is block-diagonal and each block is a pure state); this holds, e.g., for ρ_{sep}.

Theorem 4. *Let $\rho = \bigoplus_i p_i|\phi_i\rangle\langle\phi_i|$, $\sigma = \bigoplus_j q_j|\psi_j\rangle\langle\psi_j|$, where $\sum_i p_i = \sum_j q_j = 1$. Then*

$$V_F^{\text{SSR}}(\rho \otimes \sigma) = V_F^{\text{SSR}}(\rho) + V_F^{\text{SSR}}(\sigma) .$$

Proof.

$$V_F^{\text{SSR}}(\rho \otimes \sigma) = V_F^{\text{SSR}}\left(\bigoplus_{i,j} p_i q_j |\phi_i\rangle\langle\phi_i| \otimes |\psi_j\rangle\langle\psi_j|\right)$$

$$\stackrel{(*)}{=} \sum_{i,j} p_i q_j V(\phi_i \otimes \psi_j)$$

$$= \sum_i p_i V(\phi_i) + \sum_j q_j V(\psi_j)$$

$$\stackrel{(*)}{=} V_F^{\text{SSR}}(\rho) + V_F^{\text{SSR}}(\sigma) ,$$

where in $(*)$ we used the equality $V_F^{\text{SSR}}(\bigoplus_i r_i |\chi_i\rangle\langle\chi_i|) = \sum_i r_i V(\chi_i)$ with $\sum_i r_i = 1$. As subadditivity is clear from the convexity of V_F^{SSR}, we only have to show superadditivity. For an arbitrary decomposition $|\zeta_j\rangle = \sum_i u_{ji}\sqrt{r_i}|\chi_i\rangle$ of $\bigoplus_i r_i |\chi_i\rangle\langle\chi_i| = \sum_j |\zeta_j\rangle\langle\zeta_j|$ [with an isometry (u_{ji})], this follows from

$$\sum_j \frac{\langle\zeta_j|\hat{N}_A|\zeta_j\rangle^2}{\langle\zeta_j|\zeta_j\rangle} \stackrel{(a)}{=} \sum_j \frac{(\sum_i u_{ji}^* u_{ji} p_i \langle\chi_i|\hat{N}_A|\chi_i\rangle)^2}{\sum_i u_{ji}^* u_{ji} p_i}$$

$$\stackrel{(b)}{\leq} \sum_{i,j} \frac{(u_{ji}^* u_{ji} p_i \langle\chi_i|\hat{N}_A|\chi_i\rangle)^2}{u_{ji}^* u_{ji} p_i} \stackrel{(c)}{=} \sum_i p_i \langle\chi_i|\hat{N}_A|\chi_i\rangle^2 .$$

Here, we used (a) $\langle\chi_i|\chi_{i'}\rangle = \delta_{ii'}$, $\langle\chi_i|\hat{N}_A|\chi_{i'}\rangle \propto \delta_{ii'}$; (b) Eq. (7); (c) $\sum_j u_{ji}^* u_{ji} = 1$. $\qquad\square$

While it seems plausible that V_F^{SSR} is additive on all states and we did not find any counterexamples, this is apparently hard to prove. Let us note that unlike for E_F, the additivity of V_F^{SSR} is probably not related to its superadditivity. A counterexample for the superadditivity of V_F^{SSR} can easily be found [23], and the direct equivalence proof of Pomeransky [24] cannot be transferred to SiV due to the different structure of the nonlinearity.

C. Formation of qubits

In the following, we compute explicit formulas for E_F^{SSR} and V_F^{SSR} of qubits. A general bipartite two-qubit state subject to SSR is given by

$$\rho = \begin{pmatrix} w_{00} & & & \\ & w_{01} & \gamma & \\ & \gamma & w_{10} & \\ & & & w_{11} \end{pmatrix} ,$$

where $\gamma \geq 0$ (this can be achieved by local unitaries). Using the results of Wootters [25], we find $E_F(\rho) = \mathcal{E}(C)$, where $\mathcal{E}(C) = H(1/2 + \sqrt{1 - C^2}/2)$, H is the binary entropy, and the concurrence $C \equiv C(\rho)$ can be computed as
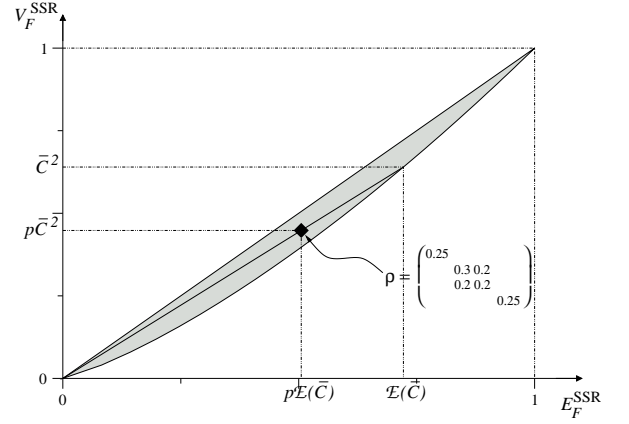
$$C = \max(0, 2\gamma - 2\sqrt{w_{00}w_{11}}) .$$

FIG. 3: Relation of p, $\bar{C}$, E_F^{SSR} and V_F^{SSR} (see Section IV C). The gray area gives the allowed range of E_F^{SSR} and V_F^{SSR} for qubits. The lower bound is obtained by plotting $\mathcal{E}(\bar{C})$ vs. $\bar{C}^2$. The point characterizing a mixed state ρ can be found by dividing the line between the origin and the point $(\mathcal{E}(\bar{C}), \bar{C}^2)$ located on the boundary at the ratio of $p : 1 - p$.

With SSR, ρ has to be built subspace by subspace, where the one-particle subspace ρ_1 is the only one which might be entangled. The concurrence for $\rho_1/\text{tr}[\rho_1]$ is

$$\bar{C} = 2\gamma/p$$

with $p = w_{01} + w_{10} = \text{tr}[\rho_1]$, and thus

$$E_F^{\text{SSR}}(\rho) = p\mathcal{E}(\bar{C}) .$$

The relation between the normal concurrence C and the SSR-concurrence $\bar{C}$ is given by the bounds $p\bar{C} - (1 - p) \leq C \leq p\bar{C}$, i.e., E_F and E_F^{SSR} are not completely independent. As $\mathcal{E}$ is concave, $E_F \leq E_F^{\text{SSR}}$, as necessary.

An optimal decomposition of ρ_1 can be found as follows. Define s as a root of $\bar{C}/2 = \sqrt{s(1 - s)}$. Then, ρ_1 can be written as a mixture of $\sqrt{s}|01\rangle + \sqrt{1 - s}|10\rangle$ and $\sqrt{1 - s}|01\rangle + \sqrt{s}|10\rangle$, and both have the desired EoE.

The same decomposition gives the optimal variance as well (note that this only holds for qubits). Therefore, observe that both states have SiV $4s(1 - s) = \bar{C}^2$, i.e., $\bar{C}^2$ is an upper bound for $V_F^{\text{SSR}}(\rho)$, and for pure states equality holds. On the other hand, $\bar{C}^2$ is convex: for any one-particle subblock $\rho_1 = p\sigma + (1 - p)\sigma'$ with off-diagonal elements $v = pw + (1 - p)w'$ it holds that $v^2 \leq pw^2 + (1 - p)w'^2$. Therefore equality holds, and

$$V_F^{\text{SSR}}(\rho) = p\bar{C}^2 . \tag{16}$$

Thus, with respect to formation 1×1 qubit states are characterized by two parameters: the weight of ρ_1, p, and the concurrence of ρ_1, $\bar{C}$. It can be checked easily that $0 \leq p, \bar{C} \leq 1$ in order for ρ to be positive. A necessary condition for separable states is $\bar{C} \leq (1 - p)/p$ (this is tight, but p, $\bar{C}$ do not tell everything about separability, cf. the inequality relating C, $\bar{C}$ given above).

Fig. 3 shows how for a particular state p and $\bar{C}$ can be determined from the E-V diagram, and Fig. 4 gives a "phase diagram" for mixed states.
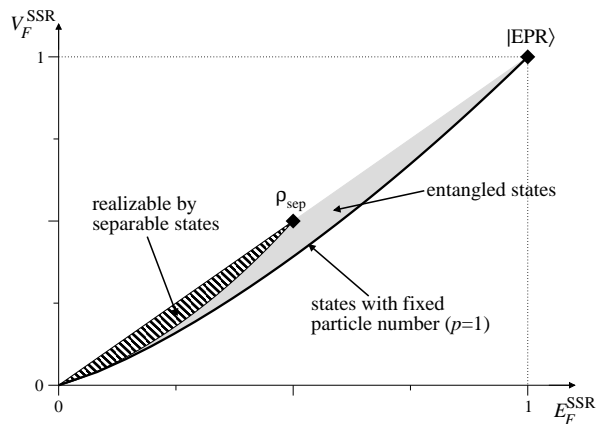
FIG. 4: Different regions of mixed states in the E-V diagram. The solid line corresponds to the states with fixed total particle number, i.e., $p = 1$. Separable states have to stay within the dashed area (although there exist entangled states as well). Note that ρ_{sep} [Eq. 14] is the "extremal separable state".

D. Distillation of nonlocal resources

In the following, we consider the problem complementary to formation: given a mixed state, is it possible to *distill* the nonlocal resources contained in this state? This distilled state could then be used to perform some nonlocal task as teleportation with high fidelity. Naturally, there exist two types of distillation protocols: the first one aims to increase the fidelity of the states being distilled with the final state, while the second returns the target state *itself* with some finite yield in the asymptotic limit.

In the following, we will focus on qubits. Without SSR, it has been shown for both types of distillation how they can be implemented: in the so-called recurrence protocol [15], both parties apply an XOR operation (a bilateral XOR or BXOR) to two copies of the state and then measure one of them; thus, on average they increase their knwoledge about the second. Hashing protocols [14], on the contrary, are aimed to asymptotically return a finite yield of pure states: by subsequent application of BXOR operations partial information about the states can be collected in a subset which is then measured; by the law of large numbers, this partial information asymptotically fully determines the remaining states.

The presence of superselection rules inposes severe restrictions on distillation procedures. It has been shown, e.g., that the entanglement contained in *one* copy of a $|\text{V-EPR}\rangle$ cannot be accessed, while for multiple copies of $|\text{V-EPR}\rangle$, all entanglement up to a logarithmic amount can be used [8], as also follows from Thm. 2. The central problem in distilling states containing SiV is that the BXOR operation is ruled out by the SSR, and there is no adequate replacement. One way to overcome this problem is to use a third copy of the state as a (imperfect) shared reference frame and to construct a three-copy protocol which probabilistically implements BXOR. Indeed, we will show that one needs three-copy protocols to distill both EoE and SiV. Unfortunately, this is of no use for the implementation of hashing protocols, as the errors of the BXOR-approximation accumulate, and each BXOR uses up the reference frame copy of the state whereas hashing would require $O(N^2)$ BXOR operations.

The existence of two distinct resources makes the field of distillation much more rich: there will occur trade-offs between the two resources in distillation, and one might even think of *spending* one resource to distill the other. For instance, we will show that it is possible to distill all separable but nonlocal states towards ρ_{sep} [Eq. (14)], and in turn, if one adds some entanglement, all the SiV contained in ρ_{sep} can be converted to a $|\text{V-EPR}\rangle$.

1. Reduction to standard states

To simplify analysis, in [14] the distillation of qubits has been considered for a standard form, namely Bell-diagonal states; any state can be made Bell-diagonal by LOCC. Yet, these operations are ruled out by the SSR, so that we have to introduce a different normal form. Therefore, consider a general bipartite qubit state with SSR

$$\rho = \begin{pmatrix} w_{00} & & & \\ & w_{01} & \gamma & \\ & \gamma^* & w_{10} & \\ & & & w_{11} \end{pmatrix}, \qquad (17)$$

where $w_{ij} \geq 0$ and $\gamma \geq 0$ (the latter can be accomplished by local unitaries). By local filtering operations [26] $F_A \propto \sqrt[4]{w_{10}w_{11}}|0\rangle\langle 0| + \sqrt[4]{w_{00}w_{01}}|1\rangle\langle 1|$, $F_B \propto \sqrt[4]{w_{01}w_{11}}|0\rangle\langle 0| + \sqrt[4]{w_{00}w_{10}}|1\rangle\langle 1|$, this can be transformed probabilistically to

$$\tilde{\rho} = \frac{1}{2(1+w)} \begin{pmatrix} w & & & \\ & 1 & v & \\ & v & 1 & \\ & & & w \end{pmatrix}. \qquad (18)$$

Here, $w = \sqrt{\frac{w_{00}w_{11}}{w_{01}w_{10}}}$ and $v = \frac{|\gamma|}{\sqrt{w_{01}w_{10}}}$. In the following, we will call this the *standard form* $\tilde{\rho}$ of a two-qubit state ρ and only consider states of this type. The standard form is Bell-diagonal and unique for each ρ, and by the reverse POVM $F'_A \propto F_A^{-1}$, $F'_B \propto F_B^{-1}$, $\tilde{\rho}$ is converted back to ρ. Thus, any state can be transformed probabilistically to its standard form and back by LOCC, and therefore the standard form of states containing EoE and SiV still contains EoE and SiV [27].

Note that the two parameters (w, v) describing the standard form $\tilde{\rho}$ are directly related to $(p, \bar{C})$ used to characterize $E_F^{\text{SSR}}(\tilde{\rho})$ and $V_F^{\text{SSR}}(\tilde{\rho})$ in Section IV C: $v = \bar{C}$ and $w = 1/p - 1$.

2. Distilling entanglement

Let us first demonstrate that it is possible to distill all entangled qubit states, as it is the case without SSR. Therefore, take two copies of an arbitrary state ρ in its standard form $\tilde{\rho}$ [Eq. (18)] and project locally onto the one-particle subspaces. The resulting state in the $\{|\hat{0}\rangle, |\hat{1}\rangle\}$-basis is

$$\hat{\rho} = \begin{pmatrix} w^2 & & & \\ & 1 & v^2 & \\ & v^2 & 1 & \\ & & & w^2 \end{pmatrix} .$$

Obviously, $\hat{\rho}$ is entangled iff $\tilde{\rho}$ is entangled iff ρ is entangled, and as $\hat{\rho}$ has constant local particle number, it can be distilled as usual [14, 15]. Therefore, it is possible to distill any entangled two-qubit state if we do not care about its SiV. Even more, if we have an infinite amount of SiV available, we can distill with the same rate as without SSR by using the SiV as a perfect reference frame.

3. Distilling separable states

Clearly, the SiV contained in separable but nonlocal states cannot be distilled, as pure states with SiV always contain entanglement. One solution to this problem is to distill towards ρ_{sep} [Eq. (14)]; we will show how this can be done (and why ρ_{sep} is a good choice) in the next subsection. Alternatively, one might try to add entanglement (e.g., $|$E-EPR$\rangle$s) and then distill the SiV of separable states to $|$V-EPR$\rangle$s.

In the following, we show how $\rho_{\text{sep}} \otimes |$E-EPR$\rangle\langle$E-EPR$|$ can be transformed to a $|$V-EPR$\rangle$ with probability $1/2$, thereby distilling all the SiV contained in ρ_{sep} to a pure state. Clearly, $|$V-EPR$\rangle$ can be obtained from an $|$E-EPR$\rangle = |01\rangle|10\rangle + |10\rangle|01\rangle$ by applying a BXOR operation, but this is ruled out by the SSR. The idea in the following is to use the SiV contained in ρ_{sep} as a shared reference frame in order to carry out the BXOR operation probabilistically. In order to see how this works, write ρ_{sep} as a mixture of $(|0\rangle + \omega|1\rangle)_A (|0\rangle + \omega|1\rangle)_B$ over all $\omega = e^{i\phi}$. If we manage to project the total state onto subspaces where ω simply gives a global phase, we can make use of the SiV of ρ_{sep}. Therefore, start with the state $|$E-EPR$\rangle\langle$E-EPR$| \otimes \rho_{\text{sep}}$ which can be written as a mixture of the states

$$|\psi_0\rangle \propto |010\rangle|100\rangle + |100\rangle|010\rangle ,$$
$$|\psi_1\rangle \propto |010\rangle|101\rangle + |100\rangle|011\rangle + |011\rangle|100\rangle + |101\rangle|010\rangle ,$$
$$|\psi_2\rangle \propto |011\rangle|101\rangle + |101\rangle|011\rangle$$

with probabilities $1/4$, $1/2$, and $1/4$. Clearly, there is no measurement which tells us which $|\psi_i\rangle$ we actually have without either destroying the entanglement contained in $|\psi_0\rangle$ and/or $|\psi_2\rangle$ or the variance contained in $|\psi_1\rangle$. As we want to extract the variance, we have to sacrifice

the EoE of $|\psi_{0,2}\rangle$: both parties do a projective measurement onto the subspaces spanned by $\{|010\rangle, |101\rangle\}$ and $\{|100\rangle, |011\rangle\}$. If the measurement outcomes match, Alice and Bob share a known state with EoE and SiV 1 which can be converted to a $|$V-EPR$\rangle$; otherwise, the entanglement is lost. Both cases are equally likely, and thus the average yield of SiV is $1/2 = V_F^{\text{SSR}}(\rho_{\text{sep}})$ which is optimal. On the other hand, we had to sacrifice half of the entanglement—there is a trade-off between the two resources.

The procedure described above can be generalized to arbitrary states, where it allows to distill the one-particle subblock. Note that if ρ is entangled, the required $|$E-EPR$\rangle$s can be distilled from ρ itself.

4. Recurrence protocols

In the following, we will look for protocols which allow to distill EoE *and* SiV. Particularly, we would like to have a protocol which allows to concentrate the SiV contained in separable states. As already mentioned at the beginning of the section, the usual recurrence protocols cannot be applied as BXOR cannot be implemented. (In fact, it is not even possible to find an operation doing a comparable job, i.e., computing the parity, only for $|0\rangle|1\rangle \pm |1\rangle|0\rangle$.) Yet, similar to the preceding subsection we can use a third copy as a shared reference frame which allows to implement the desired recurrence operation in a probabilistic way. Indeed, we will see that three-copy protocols suffice for all distillation tasks.

General N-copy recurrence protocols can be represented by local POVM operators which act on N qubits and leave one qubit (i.e., 2×2^N matrices). These operators must be realizable by SSR-compatible operations, i.e., by an N-qubit POVM, followed by a measurement of all but one qubit (omitting the measurement decreases our information about the state and thus does not help). Therefore, the POVM operators must have the shape of two adjacent rows of SSR-compatible N-qubit operations [Eq. (1)]; except normalization, this is the only condition.

Possible protocols are illustrated in Fig. 5. Any state can be brought to standard form Eq. (18) by local filtering operations and can be parametrized by a tuple (v, w), $0 \leq v \leq 1$, $0 \leq w$; the states with $v > w$ are entangled (Fig. 5a).

Given a *single* copy of $\tilde{\rho}(v, w)$, Alice and Bob can either increase w (by adding $|00\rangle\langle00| + |11\rangle\langle11|$) or decrease v and w by the same fraction (by adding $|01\rangle\langle01| + |10\rangle\langle10|$), and anything inbetween, as is illustrated in Fig. 5b. Obviously, ρ_{sep} can be transformed to any other separable state deterministically—therefore, it is indeed *the* standard separable but nonlocal state, as an EPR is for entanglement.

Let us turn our attention to two-copy protocols. As the output state will not necessarily have standard form, we have to include filtering in the local POVM operators
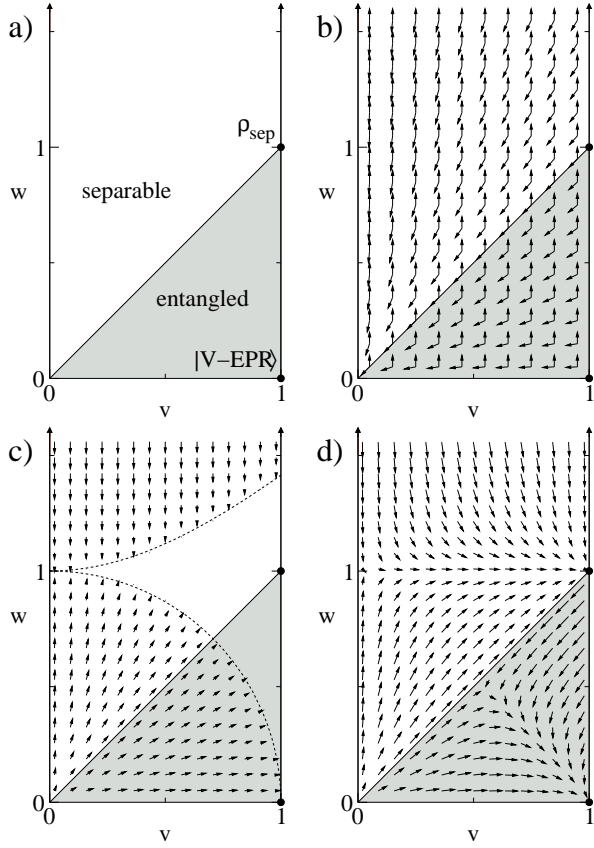
FIG. 5: **a)** Diagram characterizing mixed states according to their standard form. The entangled states are exactly those in the gray area. **b)** Transformations possible by one-copy operations: w can be increased, or w and v can be decreased simultaneously. Thereby, the $|\text{V-EPR}\rangle$ can be transformed to any state, while ρ_{sep} can generate any separable state. **c)** Additional transformations realizable by two-copy recurrence protocols. Thereby, it is not possible to reach ρ_{sep} or $|\text{V-EPR}\rangle$. **d)** Three-copy protocols allow to distill all separable states towards ρ_{sep} and all entangled ones towards $|\text{V-EPR}\rangle$.

which restricts their degrees of freedom to one complex number each, so that it is easy to check that the best protocols are given by

$$M_A = M_B \propto \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

and

$$M'_A \propto \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \quad M'_B \propto \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

The resulting transformations are $(v, w) \mapsto (v, \sqrt{\frac{1+v^2+w^2}{2}})$ and $(v, w) \mapsto \sqrt{\frac{2}{1+v^2+w^2}}(v, w)$, respectively. Fig. 5c shows where this gives an advantage over the one-copy protocol Fig. 5b. Obviously, two-copy protocols do neither allow to distill separable state to ρ_{sep} nor do they allow to distill entangled states to $|\text{V-EPR}\rangle$.

For three copies, though, the following two pairs of POVM operatos provide a way to distill all states:

$$M_A = M_B \propto \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

distills all separable states to ρ_{sep} by virtue of

$$(v, w) \mapsto \left(v + \frac{v - v^3}{1 + 2v^2 + 2w^2}, \frac{w(2 + 2v^2 + w^2)}{1 + 2v^2 + 2w^2} \right)$$

whereas

$$M'_A \propto \begin{pmatrix} 0 & 1 & 1 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{pmatrix},$$

$$M'_B \propto \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 1 & 1 & 0 \end{pmatrix}$$

distills entangled states towards a $|\text{V-EPR}\rangle$, and

$$(v, w) \mapsto \left(\frac{v(6 + 3v^2 - 2w^2)}{3 + 6v^2 + 6w^2}, \frac{w(6 - 2v^2 + 3w^2)}{3 + 6v^2 + 6w^2} \right).$$

This is illustrated in Fig. 5d.

V. SIV AS A RESOURCE

A. Introduction

In its standard form, i.e., as a singlet, EoE can be used to teleport quantum bits and thus allows to overcome the restriction to LOCC. In this section, we will show that SiV is a resource in very much the same way, namely it allows to overcome the restrictions imposed by SSR in a bipartite setting. Despite the similarities, there are some major differences. Firstly, while for EoE there only exists one standard form (the maximally entangled state depending on the dimension of the system), for SiV there exist two different standard states: singlets $|0\rangle|N\rangle + |N\rangle|0\rangle$ with SiV N^2 (as in Corollary 1) and the Gaussian distributed states with large variance (as in Theorem 2). Second, there are no pure states which carry only SiV—SiV as a resource which is independent of EoE only exists for mixed states where resources are difficult to quantify. Finally, we will find that we need an infinite amount of nonlocality in order to completely overcome the restrictions imposed by the SSR—this is fundamentally different from EoE where one ebit of entanglement is sufficient to perfectly teleport one quantum bit.

In order to demonstrate (and partly quantify) that SiV is useful to overcome the restrictions imposed by the SSR, we will use the tasks of distinguishing and teleportation. It has been shown that with SSR there exists a perfect data hiding protocol [9] which allows to encode a classical bit in a bipartite state such that it cannot be revealed by LOCC [7]. This protocol can be extended to a protocol hiding $\log N$ bits in the Fourier states

$$|\zeta_k^N\rangle = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} e^{2\pi i k n / N} |n\rangle_A |N - 1 - n\rangle_B. \qquad (19)$$

These states can be distinguished perfectly by LOCC if no SSR are present (therefore, both parties measure in the Fourier basis and compare their outcomes), but with SSR, they become totally indistinguishable (see Theorem 5 below).

The second task we use to show that SiV is a resource is teleportation of a state with nonconstant local particle number: Alice holds one half of a state $|\phi\rangle_{AC}$ which she wants to teleport to Bob using an in general mixed helper state ρ_{AB}. Clearly, one ebit of EoE is necessary for this task, but if $V(|\phi\rangle) > 0$, also SiV is needed [7]. We will show that one ebit of EoE is still sufficient, but the amount of SiV has to grow superlinearly with $V(|\phi\rangle)$ and is infinite for perfect teleportation.

B. A general protocol

Let us first quote a Theorem from [7] which will be very useful in the following.

Theorem 5 ([7]). *In the presence of superselection rules, the states ρ and $\mathcal{N}_{A|B}(\rho)$ cannot be distinguished by LOCC. Here, $\mathcal{N}_{A|B}$ is the "dephasing map"*

$$\mathcal{N}_{A|B}(\rho) = \sum_{n_A, n_B} P_{n_A}^A \otimes P_{n_B}^B \rho P_{n_A}^A \otimes P_{n_B}^B \ ,$$

with $P_{n_X}^X$ the local projector onto the subspace with n_X particles.

By this theorem, we can highly restrict the class of allowed protocols. Let us show this for the task of distinguishing, where Alice and Bob initially share $\rho = |\zeta_k^N\rangle\langle\zeta_k^N| \otimes \sigma$ [cf. Eq. (19)], and they have to determine k. At the end of the protocol, Alice and Bob get an answer k' according to a probability distribution $\{p_{k'}\}$. But if they had started with $\mathcal{N}_{A|B}(\rho)$ instead, Theorem 5 tells us that the probability distribution of their outcomes would have been just the same. Therefore, Alice and Bob can start their protocol by measuring their particle number operators $\hat{N}_A$ and $\hat{N}_B$—if they discard their outcomes, they just implemented $\mathcal{N}_{A|B}$, and their knowledge of N_A and N_B will not affect the *average* probability distribution which is solely relevant unless the figure of merit is nonlinear. The same holds for the teleportation scenario with respect to the partition $A|BC$, i.e., in this case only Alice is allowed to measure her particle number (this map is actually weaker than $\mathcal{N}_{A|BC}$). Note that for a pure state, measuring $\hat{N}_A$ also determines N_{BC} (and thus implements $\mathcal{N}_{A|BC}$), which is different in the mixed state case and closely connected to the fact that mixed states alone are not sufficient for teleportation.

C. Pure states

Assume Alice wants to teleport her share of the state

$$|\phi\rangle = \sum_n \alpha_n |n\rangle_A |-n\rangle_C$$

to Bob using

$$|\psi\rangle = \sum_m \beta_m |m\rangle_A |-m\rangle_B \ .$$

Here, we use a simplified notation, where $-\infty < n, m < \infty$, $\sum |\alpha_n|^2 = \sum |\beta_m|^2 = 1$, and the support of the α_n, β_m is bounded below such that the particle number can be made positive by adding ancillas. As shown before, Alice can start any protocol by measuring $N_A = K$, yielding

$$\sqrt{p_K}|\chi_K\rangle_{ABC} = \sum_{n+m=K} \alpha_n \beta_m |n, m\rangle_A |-n\rangle_C |-m\rangle_B \tag{20}$$

with included probability p_K. If Alice now measures in the Fourier basis and communicates her result, the originally tripartite state can be reconstructed by Bob and Charlie; this strategy is optimal as no information is lost and the state gets less nonlocal. Up to shifts in the particle number, the state is then

$$\sqrt{p_K}|\chi_K\rangle_{BC} = \sum_n \alpha_n \beta_{K-n}|n\rangle_B |-n\rangle \ .$$

We will use the average entanglement fidelity as the figure of merit,

$$\bar{F} = \left\langle \sum_K p_K \left|\langle\phi|\chi_K\rangle\right|^2 \right\rangle = \sum_\Delta \Pi(\Delta)C(\Delta)$$

where $\Pi(\Delta) = \sum_n \langle p_n p_{n+\Delta}\rangle$ ($p_n = |\alpha_n|^2$) and $C(\Delta) = \sum_m \beta_m^* \beta_{m-\Delta}$. The average $\langle\cdot\rangle$ is taken over all states ϕ, where for teleportation we assume a unitarily invariant distribution. It is straightforward to check that local filtering operations cannot increase $\bar{F}$. Also, for the task of distinguishing it can be shown that $\bar{F}$ gives the optimal success probability for the inconclusive case [28]. For distinguishing, $\Pi_D(\Delta) = \max(N - |\Delta|, 0)/N^2$, while for teleportation, $\Pi_T(\Delta) = [\max(N - |\Delta|, 0) + \delta_{\Delta,0}]/N(N + 1)$ [29]. In both cases, $\alpha_n \neq 0$ for $n = 0, \ldots, N - 1$.

We will analyze two natural types of helper states: states with constant distribution $\beta_m = 1/\sqrt{M}$, $m = 0, \ldots, M - 1$, and states with Gaussian distribution with variance $V(\psi)$. One finds $C_C(\Delta) = \max(M - |\Delta|, 0)/M$ resp. $C_G(\Delta) = \exp[-\Delta^2/2V] \approx 1 - \Delta^2/2V$. The resulting error probabilities for all four cases are given in Table I. Note that for the Gaussian distributed $|\psi\rangle$, in both cases

$$p_{\mathrm{err}} = \frac{\langle V(\phi)\rangle}{4V(\psi)}$$

holds, i.e., the error probability is given by the *ratio* of the variances. (Actually, this even holds without taking the average over ϕ.)

In all cases, the error vanishes only if the size of the helper state grows superlinearly with the size of the unknown state; thus, the scaling of SiV as a resource is

helper	task	
	distinguish	teleport
constant	$p_{\text{err}} = \frac{(N+1)(N-1)}{3MN}$	$p_{\text{err}} = \frac{N}{3M}$
Gaussian	$p_{\text{err}} = \frac{(N+1)(N-1)}{12V(\psi)}$	$p_{\text{err}} = \frac{N(N-1)}{12V(\psi)}$

TABLE I: Error probabilities for distinguishing and teleportation where the helper state is either a maximally entangled state with Schmidt number N or a Gaussian distributed state with variance $V(\psi)$.

unfavorable compared to the behaviour of EoE. This is a direct consequence of the direct sum structure in (3) which is opposed to the tensor product structure leading to EoE: while with a tensor product structure, N particles generate a 2^N-dimensional Hilbert space, for the direct sum structure the underlying space only has dimension $N+1$. This also holds for mixed states, where this is the size of the largest coherent subspace. For the same reason, the data hiding scheme Eq. (19) is optimal in the sense that the *available* Hilbert space has only dimension N.

D. Mixed states

Let us now demonstrate that separable mixed states with SiV can also be used as a shared reference frame [7]. First, we demonstrate how Alice and Bob can use the state ρ_{sep} to distinguish the states $|01\rangle \pm |10\rangle$. By very much the same argument as before Alice and Bob can start their protocol by measuring their local particle number. By *adding* their outcomes, Alice and Bob immediately know whether they are dealing with the $|0\rangle|0\rangle/|1\rangle|1\rangle$ part of ρ_{sep} or with the $|\text{V-EPR}\rangle$. In the first case all information is lost while in the second case they can just proceed as if they had started with $|\text{V-EPR}\rangle$ itself. This case occurs with probability $1/2$, i.e., all the SiV contained in ρ_{sep} can be used. Clearly, this protocol can not be used for teleportation as $\hat{N}_{BC}$ cannot be implemented locally.

Let us now show that separable but nonlocal states can be used to overcome locality constraints arbitrarily well, i.e., they can serve as arbitrarily precise reference frames. Therefore, we use the separable state [7, 30]

$$\rho_{\text{coh}}(\alpha) = \int \frac{\mathrm{d}\phi}{2\pi} |\alpha e^{i\phi}\rangle\langle\alpha e^{i\phi}| \otimes |\alpha e^{i\phi}\rangle\langle\alpha e^{i\phi}|$$

where for $\alpha > 0$,

$$|\alpha e^{i\phi}\rangle = e^{-\alpha^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} e^{in\phi}$$

is a coherent state with amplitude $\alpha e^{i\phi}$. It has been shown [7] that for $\alpha \to \infty$, $\rho_{\text{coh}}(\alpha)$ can be used to distinguish $|01\rangle \pm |01\rangle$ with arbitrary precision. In the following,

we will show that this state together with one $|\text{E-EPR}\rangle$ can be used to perfectly teleport a state with nonconstant local particle number and therefore may serve as an arbitrarily precise reference frame.

First, let us use Theorem 4 to show that this state has indeed infinite SiV for $\alpha \to \infty$. Therefore, it is enough to note that

$$\rho_{\text{coh}}(\alpha) = \sum_{N=0}^{\infty} p_N |\theta_N\rangle\langle\theta_N| ; \quad p_N = e^{-2\alpha^2} \frac{(2\alpha^2)^N}{N!}$$

$$|\theta_N\rangle = \frac{1}{\sqrt{2^N}} \sum_{n=0}^{N} \binom{N}{n}^{1/2} |n, N-n\rangle ,$$

and thus $V_F^{\text{SSR}}(\rho_{\text{coh}}(\alpha)) = V_c^{\text{SSR}}(\rho_{\text{coh}}(\alpha)) = \alpha^2/2 \to \infty$ for $\alpha \to \infty$. In is interesting to note that each of the $|\theta_N\rangle$ approximates a state with Gaussian distribution such that $\rho_{\text{coh}}(\alpha)$ might be considered as the EoE-free mixed state version of Gaussian distributed states.

In order to see how a mixed state can be used to teleport, let Alice and Charlie initially share $|\phi\rangle = \alpha|01\rangle + \beta|10\rangle$ (the proof is completely analogous for qu-d-its), and assume Alice wants to teleport her share to Bob. Therefore, Alice and Bob are provided with an $|\text{E-EPR}\rangle_{AB}$ and with some mixed state

$$\rho = \sum_{\substack{n,m,n',m' \\ n+m=n'+m'}} \rho_{n,m}^{n',m'} |n\rangle_A\langle n'| \otimes |m\rangle_B\langle m'| , \qquad (21)$$

where the condition $n+m = n'+m'$ comes from the SSR, Eq. (1). For simplicity, let us assume that all $\rho_{n,m}^{n',m'}$ are nonnegative. Alice once more starts by measuring her local particle number operator on $|\phi\rangle\langle\phi| \otimes \rho$. (In this step, we do not have to care about the $|\text{E-EPR}\rangle$ which has constant local particle number.) For a measurement outcome n, the resulting state (probability included) is

$$\sum_m \Big[|\alpha|^2 \rho_{n,m-1}^{n,m-1} |0,n\rangle_A\langle 0,n| \otimes |m-1\rangle_B\langle m-1| \otimes |1\rangle_C\langle 1|$$

$$+ |\beta|^2 \rho_{n-1,m}^{n-1,m} |1,n-1\rangle_A\langle 1,n-1| \otimes |m\rangle_B\langle m| \otimes |0\rangle_C\langle 0|$$

$$+ \alpha\beta^* \rho_{n,m-1}^{n-1,m} |0,n\rangle_A\langle 1,n-1| \otimes |m-1\rangle_B\langle m| \otimes |1\rangle_C\langle 0|$$

$$+ \alpha^*\beta \rho_{n-1,m}^{n,m-1} |1,n-1\rangle_A\langle 0,n| \otimes |m\rangle_B\langle m-1| \otimes |0\rangle_C\langle 1| \Big]$$

As Alice's share now has constant particle number and lies within a two-dimensional subspace, she can use the $|\text{E-EPR}\rangle_{AB}$ to teleport her share to Bob. If we label the two teleported basis states $|\hat{a}\rangle = |0,n\rangle$, $|\hat{b}\rangle = |1,n-1\rangle$, Bob and Charlie then share the state

$$\sum_m \Big[|\alpha|^2 \rho_{n,m-1}^{n,m-1} |\hat{a}, m-1\rangle_B\langle\hat{a}, m-1| \otimes |1\rangle_C\langle 1|$$

$$+ |\beta|^2 \rho_{n-1,m}^{n-1,m} |\hat{b}, m\rangle_B\langle\hat{b}, m| \otimes |0\rangle_C\langle 0|$$

$$+ \alpha\beta^* \rho_{n,m-1}^{n-1,m} |\hat{a}, m-1\rangle_B\langle\hat{b}, m| \otimes |1\rangle_C\langle 0|$$

$$+ \alpha^*\beta \rho_{n-1,m}^{n,m-1} |\hat{b}, m\rangle_B\langle\hat{a}, m-1| \otimes |0\rangle_C\langle 1| \Big]$$

Bob now projects onto the subspaces spanned by the pairs of states $|0_m\rangle \equiv |\hat{a}, m-1\rangle$ and $|1_m\rangle \equiv |\hat{b}, m\rangle$ and obtains

$$
\begin{aligned}
& |\alpha|^2 \rho_{n,m-1}^{n,m-1} |0\rangle_B \langle 0| \otimes |1\rangle_C \langle 1| \\
+\ & |\beta|^2 \rho_{n-1,m}^{n-1,m} |1\rangle_B \langle 1| \otimes |0\rangle_C \langle 0| \\
+\ & \alpha\beta^* \rho_{n,m-1}^{n-1,m} |0\rangle_B \langle 1| \otimes |1\rangle_C \langle 0| \\
+\ & \alpha^*\beta \rho_{n-1,m}^{n,m-1} |1\rangle_B \langle 0| \otimes |0\rangle_C \langle 1| \qquad (22)
\end{aligned}
$$

(where we omitted the subscript m). By looking at the average fidelity with the original state, we find that the error vanishes iff

$$
\sum_{n,m} \rho_{n,m-1}^{n,m-1} = \sum_{n,m} \rho_{n-1,m}^{n-1,m} = \sum_{n,m} \rho_{n-1,m}^{n,m-1} . \qquad (23)
$$

Since ρ is positive this implies that $\rho_{n,m-1}^{n,m-1} \approx \rho_{n-1,m}^{n-1,m} \approx \rho_{n-1,m}^{n,m-1}$ for most n, m, as one would expect from Eq. (22). It is straightforward to check that Eq. (23) holds for $\rho_{\mathrm{coh}}(\alpha)$ for $\alpha \to \infty$, and that the 2×2 subblocks of the density matrix really approximate pure states.

One might expect that $N \to \infty$ copies of ρ_{sep} could be used just the same way, but the situation is quite different: filtering operations which bring $\rho_{\mathrm{sep}}^{\otimes N}$ into a form (21) destroy the off-diagonal elements of the density matrix with high probability so that (23) cannot be satisfied; therefore it is questionable whether multiple copies of ρ_{sep} can be used as an arbitrarily precise reference frame. On the other hand, this is not so much different from the pure state scenario: while multiple copies of a $|\text{V-EPR}\rangle$ might indeed be used as a perfect reference frame, these states carry an amount of entanglement which grows *linearly* with the precision of the reference frame, whereas a single Gaussian distributed state with large SiV only has *logarithmic*—and thus in some sense vanishing—entanglement and is therefore much closer to the case of separable reference frames.

Let us note that the teleportation scenario can be altered by joining B and C. This is no longer teleportation, of course, and can be accomplished by LOCC without SSR. On the other hand, it is still an impossible task if SSR are present and is thus suitable to characterize mixed states as reference frames without the need for additional entanglement.

E. Hiding quantum states

Let us close by showing that the data hiding protocol given in [7] resp. its extension Eq. (19) can be used to construct a mixed state scheme to hide quantum data as well. At a first glance, one might try to encode the two degrees of freedom of a qubit in the phases of the state $|02\rangle + e^{i\phi}|11\rangle + e^{i\phi'}|20\rangle$, but this cannot be accomplished by a linear map. Therefore, we encode the qubit $\alpha|01\rangle + \beta|10\rangle$ in one of the states $|\phi_0\rangle = \alpha|01\rangle + \beta|10\rangle$, $|\phi_1\rangle = \beta|01\rangle + \alpha|10\rangle$ with equal probabilities which is then

distributed between Alice and Bob. Additionally, Alice and Bob are provided with a state $|\psi_{0/1}\rangle = |02\rangle \pm |20\rangle$ which encodes the state Alice and Bob actually share. Thus, Alice and Bob share a state which they cannot distinguish from the totally mixed state by LOCC (Theorem 5), but they can perfectly recover the original qubit if they join. This scheme can be extended to hide N-level quantum states using one of the states

$$
|\phi_k\rangle = \sum_{n=0}^{N-1} \alpha_{n+k \bmod N} |n, N-1-n\rangle ; \quad k = 0, \ldots, N-1 .
$$

Together with the state encoding k, $N^2 - 1$ particles are needed, and the associated Hilbert space dimension is N^2.

VI. CONCLUSIONS

Adding restrictions to the operations permissible on a quantum system gives rise to a new resource which in turn allows to overcome this restriction. The restriction to LOCC, for example, leads to EoE as a nonlocal resource. Adding SSR to a bipartite system leads to an additional resource, the superselection induced variance SiV. We could show that SiV and EoE together completely characterize bipartite states in the asymptotic limit. Thereby, two different kind of standard forms arise, namely singlets and Gaussian distributed states with logarithmic EoE.

The search for states which only carry SiV led us to mixed states, where we considered entanglement and variance of formation. We could show that the concept of entanglement does not have to be changed and thus there exist states which carry SiV but no EoE, and we provided explicit formulas for the case of qubits. As to distillation, we could show that both EoE and SiV can be distilled, and we provided various ways to do that. Thereby, we found that there exist mixed standard states for SiV which do not carry EoE. While it is possible to extend recurrence protocols such that they work with SSR by using a third copy as a reference frame, it is unlikely that protocols with asymptotic yield work.

Finally, we showed that SiV is a resource which allows to overcome the restrictions imposed by the SSR, but we also saw that there are fundamental differences to EoE as the size of the reference frame has to grow superlinearly with the problem size, which is due to direct sum structure of the underlying Hilbert space.

Acknowledgments

APPENDIX: PROOF OF EQ. (15)

In order to show Eq. (15), we need the inequality $S(p_i \rho_i) \leq p_i S(\rho_i) + H(p_i)$ (see, e.g., [21] for a proof). Furthermore, note that $P_n = \sum_{i=0}^{n} P_i^A \otimes P_{n-i}^B$. Toghether, this gives the estimate

$$
E\left(\frac{P_n|\psi\rangle}{\sqrt{\langle\psi|P_n|\psi\rangle}}\right) = S\left(\frac{\text{tr}_B \sum_{i=0}^{n} P_i^A \otimes P_{n-i}^B |\psi\rangle\langle\psi| P_i^A \otimes P_{n-i}^B}{\langle\psi|P_n|\psi\rangle}\right)
$$
$$
\leq \sum_{i=0}^{n} \frac{\langle\psi|P_i^A \otimes P_{n-i}^B|\psi\rangle}{\langle\psi|P_n|\psi\rangle} S\left(\frac{\text{tr}_B P_i^A \otimes P_{n-i}^B |\psi\rangle\langle\psi| P_i^A \otimes P_{n-i}^B}{\langle\psi|P_i^A \otimes P_{n-i}^B|\psi\rangle}\right) + H\left(\left\{\frac{\langle\psi|P_i^A \otimes P_{n-i}^B|\psi\rangle}{\langle\psi|P_n|\psi\rangle}\right\}_{i=0}^{N}\right) .
$$

Clearly, the Shannon entropy H is bounded by $\log(n+1) \leq \log(N+1)$, and thus the l.h.s. of Eq. (15), i.e., the entanglement averaged over n, is bounded by

$$
\sum_{n=0}^{N} \sum_{i=0}^{n} \langle\psi|P_i^A \otimes P_{n-i}^B|\psi\rangle \, S\left(\frac{\text{tr}_B P_i^A \otimes P_{n-i}^B |\psi\rangle\langle\psi| P_i^A \otimes P_{n-i}^B}{\langle\psi|P_i^A \otimes P_{n-i}^B|\psi\rangle}\right) + \log[N+1] .
$$

The sum can be extended to $i = 0, \ldots, N$, $n - i = 0, \ldots, N$ as $|\psi\rangle$ has at most N particles, and by the convexity of the von Neumann entropy, Eq. (15) follows.

---

[1] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996), quant-ph/9511030.

[2] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[3] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).

[4] P. Zanardi, Phys. Rev. Lett. **87**, 077901 (2001), quant-ph/0103030; P. Zanardi, D. Lidar, and S. Lloyd, Phys. Rev. Lett. **92**, 060402 (2004), quant-ph/0308043.

[5] H. Barnum, E. Knill, G. Ortiz, and L. Viola, Phys. Rev. A **68**, 032308 (2003), quant-ph/0207149; H. Barnum, E. Knill, G. Ortiz, R. Somma, and L. Viola, Phys. Rev. Lett. **92**, 107902 (2004), quant-ph/0305023.

[6] S. Popescu, personal communication.

[7] F. Verstraete and J. I. Cirac, Phys. Rev. Lett. **91**, 010404 (2003), quant-ph/0302039.

[8] H. M. Wiseman and J. A. Vaccaro, Phys. Rev. Lett. **91**, 097902 (2003), quant-ph/0210002; S. D. Bartlett and H. M. Wiseman, Phys. Rev. Lett. **91**, 097903 (2003), quant-ph/0303140; H. M. Wiseman, S. D. Bartlett, and J. A. Vaccaro, quant-ph/0309046; J. A. Vaccaro, F. Anselmi, and H. M. Wiseman, Int. J. Quant. Inf., **1**, 427 (2003), quant-ph/0311028.

[9] B. M. Terhal, D. P. DiVincenzo, and D. W. Leung, Phys. Rev. Lett. **86**, 5807 (2001).

[10] A. Kitaev, D. Mayers, and J. Preskill (2003), quant-ph/0310088.

[11] S. D. Bartlett, T. Rudolph, and R. W. Spekkens (2004), quant-ph/0403161.

[12] N. Schuch, F. Verstraete, and J. Cirac, Phys. Rev. Lett. **92**, 087904 (2004), quant-ph/0310124.

[13] M. Nielsen, Phys. Rev. Lett. **83**, 436 (1999), quant-ph/9811053.

[14] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996), quant-ph/9604024.

[15] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, Phys. Rev. Lett. **76**, 722 (1996), quant-ph/9511027.

[16] D. Jonathan and M. B. Plenio, Phys. Rev. Lett. **83**, 1455 (1999), quant-ph/9903054.

[17] If one includes ancillas, the Theorem only holds up to shifts in the local particle number performed on the output states, i.e., Eq. (5) has to be replaced by $\exists \nu_i \in \mathbb{N}$ $\forall n = 0, \ldots, N : \boldsymbol{\lambda}^n \prec \sum_i p_i \boldsymbol{\mu}_i^{n+\nu_i}$. Formally, up to local unitaries each state is then described by an *equivalence class* of SSR-ordered Schmidt vectors which are equal up to a shift in the particle number, and there have to exist vectors in these equivalence classes which satisfy Eq. (5). The proof transfers directly if one replaces $\hat{\psi}^n$ by $\hat{\psi}^{n+\nu_i}$.

[18] H.-K. Lo and S. Popescu, Phys. Rev. A **63**, 022301 (2001), quant-ph/9707038.

[19] G. Vidal, J. Mod. Opt. **47**, 355 (2000), quant-ph/9807077.

[20] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (Wiley-Interscience, 1991).

[21] M. A. Nielsen and I. A. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, 2000).

[22] P. M. Hayden, M. Horodecki, and B. M. Terhal, J. Phys. A **34**, 6891 (2001), quant-ph/0008134.

[23] E.g, for class of 2×2 qubit states given by $|\phi\rangle = \alpha|00\rangle_A|11\rangle_B + \beta|01\rangle_A|10\rangle_B + \beta|10\rangle_A|01\rangle_B + \alpha|11\rangle_A|00\rangle_B$ with $\alpha = \sqrt{p/2}$, $\beta = \sqrt{(1-p)/2}$, and $p < 1/2$, V_F^{SSR} is not superadditive with respect to the two subsystems, since $V(|\phi\rangle) = 4p$ and $V_F^{\text{SSR}}(\text{tr}_i[|\phi\rangle\langle\phi|]) = 4p(1-p)$.

[24] A. Pomeransky, Phys. Rev. A **68**, 032317 (2003), quant-ph/0305056.

[25] W. K. Wootters, Phys. Rev. Lett. **80**, 2245 (1998), quant-ph/9709029.

[26] F. Verstraete, J. Dehaene, and B. DeMoor, Phys. Rev. A

64, 010101(R) (2001), quant-ph/0011111.

[27] Some special cases for ρ have to be considered separately. Note that if $v = 0$ ρ can be created by LOCC, and $v = 0$ follows if $w_{01} = 0$ or $w_{10} = 0$. If $w_{00} = w_{11} = 0$, filtering still works in both directions if w_{00} and w_{11} are deleted from the filtering operators. In case $w_{00} = 0$, $w_{11} > 0$ or vice versa, the situation gets more complicated. In order to distill ρ, one adds $|00\rangle\langle00|$ with some weight which does not destroy the entanglement; then, ρ can be distilled to $|$V-EPR$\rangle$, from where it can be easily reconstructed.

[28] A. Chefles, Contemporary Physics **41**, 401 (2000), quant-ph/0010114.

[29] K. Banaszek, Phys. Rev. A **62**, 024301 (2000), quant-ph/0002088.

[30] T. Rudolph and B. C. Sanders, Phys. Rev. Lett. **87**, 077903 (2001), quant-ph/0103147.