Quantifying the resource of sharing a reference frame

S.J. van Enk[b,c]
[b] *Bell Labs, Lucent Technologies*
600 Mountain Ave,
Murray Hill, NJ 07974
[c] *Institute for Quantum Information*
California Institute of Technology
Pasadena, CA 91125
(Dated: February 1, 2008)

We define a new quantity called *refbit*, which allows one to quantify the resource of sharing a reference frame in quantum communication protocols. By considering both asymptotic and nonasymptotic protocols we find relations between *refbits* and other communication resources. We also consider the same resources in encoded, reference-frame independent, form. This allows one to rephrase and unify previous work on phase references, reference frames, and superselection rules.

I. INTRODUCTION

The roles that reference frames play in communication protocols have attracted a lot of attention in recent times. Many aspects related to the transmission of a direction in space by quantum particles have been analyzed in detail, see for instance Refs. [1]. It was also pointed out that both classical and quantum communication are possible without sharing a reference frame by encoding information in particular invariant subspaces [2]. Moreover, several papers have discussed the relation between reference frames (or more generally, phase references) and super-selection rules, and their role in quantum communication [3, 4]. Finally, sharing a secret reference frame as a cryptographic resource was analyzed in [5].

In most of the work mentioned above a reference frame is assumed to be either fully present or fully absent. The present paper attempts to quantify the partial presence of a phase reference. Ref. [3], too, quantifies a resource that can substitute for a phase reference. That quantity applies to one case of two considered in the present paper (see Section III), and describes in fact two different resources, the *ebit* and the *refbit*, which are similar in certain contexts but different in others. The *ebit* and other resources, such as a unit of coherent communication, a *cobit*, were defined and analyzed in Ref. [6], but under the implicit assumption that the communicating parties share a reference frame. Here we modify those definitions to explicitly take into account the absence of a shared reference frame, and in addition we introduce a unit of sharing a phase reference, a *refbit*. The formalism presented here is an alternative, and hopefully useful, way of formulating the role reference frames play in communication protocols. Indeed, by following the methods of [6] we can rephrase and unify results from several previous papers on reference frames and superselection rules, such as [3] and [7] (see also [8]). For example, we will introduce encoded, phase-reference independent, versions of the resources, such as an *Ebit*, which we will always denote by capitalizing the word used for the unencoded resource. The relations between *ebits* and *Ebits* clarify the various measures of entanglement used in [7], and also how quantum data hiding [3] in the presence of superselection rules works, thus unifying those two results. The encoding used is inspired by that of Ref. [2], but is different as our communication model, presented below, is different.

Since notation can be confusing as various terms, such as qubits and ebits, are used in different contexts with different meanings, we start out by clarifying the notation used in this paper.

II. NOTATION

A two-level atom or a polarized photon can act as a physical qubit. On the other hand, the *qubit* used in this paper (and in Ref. [6]) is a communication resource, and is equivalent to sending a physical qubit over a noiseless channel (this will be made more precise in Section IV). In order to distinguish the two types of "qubits", we will always write the communication resource *qubit* in italic, the other type of "qubit" will always be prefaced by the word "physical" and written in roman.

Somewhat similarly, the ebit is known as a unit of entanglement. It can be used to quantify the amount of entanglement in any bipartite state. The *ebit* used in this paper (and also in [6]) is, again, a communication resource. For example, when Alice and Bob are engaged in some quantum communication protocol, then an *ebit* is the resource of Alice and Bob sharing an entangled state of a particular form. That entangled state contains one ebit of entanglement.

Finally, the following notation should be clear by now: a classical bit is a unit of classical information, the *cbit* in the present paper is a communication resource and corresponds to sending a classical bit over a noiseless channel.

III. COMMUNICATION MODEL

Assume that Alice and Bob agree on the definition of the qubit states $|0\rangle$ and $|1\rangle$, but not on the definition of the phase ϕ in superpositions of the form

$$\sin\alpha|0\rangle + \cos\alpha e^{i\phi}|1\rangle.$$

For them to agree on the value of ϕ they would have to share a phase reference.

This model corresponds to Alice and Bob communicating with either photon number states, with $|0\rangle$ and $|1\rangle$ denoting states containing no and one photon in one particular mode [13], or with polarized single photons, with $|0\rangle$ and $|1\rangle$ denoting left-hand and right-hand circular polarization. The phase references needed in these two cases are a synchronized clock and a spatial reference frame, respectively [14].

Both Alice and Bob are assumed to have local phase references at their disposal, which define local phases ϕ_A and ϕ_B, respectively. It is important to note that these two phases in turn are defined only with respect to another, fictituous phase reference, that we may assume to be in the hands of a third party. For instance, in the context of cryptographic protocols we may assume this third party is an eavesdropper. Neither Alice nor Bob are aware of the values of ϕ_A and ϕ_B. Thus, the third party reference frame has a privileged role.

Those who believe that superselection rules might forbid coherent superpositions of $|0\rangle$ and $|1\rangle$ [15] may prefer the following, alternative, cumbersome, but in the end equivalent, formulation: The fictituous third party has a state of the form

$$\int \frac{\mathrm{d}\phi}{2\pi}((|0\rangle + \exp(i\phi)|1\rangle)(\langle 0| + \exp(-i\phi)\langle 1|))^{\otimes N},$$

with $N \to \infty$. In spite of appearances this state contains no coherent superpositions of $|0\rangle$ and $|1\rangle$. Now whenever a phase between $|0\rangle$ and $|1\rangle$ appears in some equation this phase is understood to be relative to the dummy phase ϕ. For example, the equivalent of "Alice having a state $|0\rangle_A + \exp(i\phi_A)|1\rangle_A$" is then that the joint state of the third party and Alice's qubit is

$$\int \frac{\mathrm{d}\phi}{2\pi}((|0\rangle + \exp(i\phi)|1\rangle)(\langle 0| + \exp(-i\phi)\langle 1|))^{\otimes N} \otimes$$
$$(|0\rangle + \exp(i(\phi+\phi_A))|1\rangle)(\langle 0| + \exp(-i(\phi+\phi_A))\langle 1|).$$

One can define in a similar way what it means for Alice and Bob to have their own phase references: large collections of physical qubits with phases $\phi+\phi_A$ or $\phi+\phi_B$, respectively.

In any case, Alice and Bob can perform any local operation they like, except that there will always be extra phase factors $\exp(i\phi_A)$ or $\exp(i\phi_B)$ appearing in front of the states $|1\rangle_A$ and $|1\rangle_B$. For example, consider the Hadamard transformation. When Alice performs her version of that transformation, she actually performs H_A:

$$\begin{aligned} |0\rangle &\mapsto |0\rangle + \exp(i\phi_A)|1\rangle \\ |1\rangle &\mapsto \exp(-i\phi_A)|0\rangle + |1\rangle, \end{aligned} \tag{1}$$

as described from the third-party reference frame. Similarly, when she performs her local version of a controlled-NOT, she actually performs CNOT_A:

$$\begin{aligned} |0\rangle|0\rangle &\mapsto |0\rangle|0\rangle \\ |0\rangle|1\rangle &\mapsto |0\rangle|1\rangle \\ |1\rangle|0\rangle &\mapsto \exp(i\phi_A)|1\rangle|1\rangle \\ |1\rangle|1\rangle &\mapsto \exp(-i\phi_A)|1\rangle|0\rangle. \end{aligned} \tag{2}$$

The three Pauli operations become

$$\begin{aligned} Z_A &= Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\ X_A &= \begin{pmatrix} 0 & \exp(i\phi_A) \\ \exp(-i\phi_A) & 0 \end{pmatrix} \\ Y_A &= \begin{pmatrix} 0 & \exp(i\phi_A) \\ -\exp(-i\phi_A) & 0 \end{pmatrix} \end{aligned} \tag{3}$$

If we picture a (Bloch) sphere representing a qubit, then Alice and Bob agree on the north and south poles, they agree on the latitude of all points on the sphere, but not on the longitude. They can perfectly define rotations around the polar axis, but not around any other rotation axis.

IV. DEFINITIONS OF RESOURCES

In order to define various resources such as *ebits* and *qubits*, we follow Ref. [6], but with the appropriate modifications to reflect the assumptions of the communication model defined in the preceding Section. Ref. [6] implicitly assumed Alice and Bob do share a phase reference. The first three definitions given below refer to resources that are *sent* from one party to the other (and in the definitions we always consider Alice the sender and Bob the receiver). The last three definitions define resources *shared* by Alice and Bob.

Before we give the definitions it is perhaps useful to point out the following. Under the assumption of a shared reference frame the definition of an *ebit* (as in [6]), for example, includes a more general class of entangled states than the ones considered below. Moreover, entangled states are more powerful resources in the presence of a reference frame. Indeed, that was one point of Refs. [3] and [7]. The *ebit* as defined in the present paper is less powerful, but the *Ebit* defined later on is much more similar to the quantity defined in [6].

1. The most powerful resource is a *qubit*, that is, one use of a perfect quantum communication channel. It is the ability to send any physical qubit from Alice to Bob, i.e.,

   $$a|0\rangle_A + b|1\rangle_A \mapsto a|0\rangle_B + b|1\rangle_B.$$

   Here the coefficient b does not necessarily contain an explicit phase factor $\exp(i\phi_A)$ as the physical qubit may have been handed to Alice by a third party (this may be relevant in a teleportation protocol, for instance).

2. A *cobit* is the ability to perform

$$\begin{aligned}|0\rangle_A &\mapsto |0\rangle_A|0\rangle_B,\\ |1\rangle_A &\mapsto \exp(i\phi_A)|1\rangle_A|1\rangle_B.\end{aligned}$$

Here the phase factor $\exp(i\phi_A)$ does always appear. This definition is basis-dependent, as it singles out the $|0\rangle, |1\rangle$ basis. This basis dependence is necessary as the *cobit* is defined by a cloning-like operation.

3. A *cbit*, corresponds to one use of a classical communication channel, which can be described by the process

$$\begin{aligned}|0\rangle_A &\mapsto |0\rangle_E|0\rangle_B,\\ |1\rangle_A &\mapsto \exp(i\phi_A)|1\rangle_E|1\rangle_B,\end{aligned}$$

where E refers to the environment, assumed unobservable by either Alice or Bob, but possibly observable by an eavesdropper. In any protocol involving *cbits*, we thus assume that Alice and Bob trace out the environment.

4. The following definition of an *ebit* is chosen such that both a single *qubit* and a single *cobit* can be used to generate an *ebit*, a bipartite entangled state of a particular form, shared by Alice and Bob: Alice, starting out with the state $|0\rangle \pm \exp(i\phi_A)|1\rangle$, can use a *cobit* to produce

$$|0\rangle_A|0\rangle_B \pm \exp(2i\phi_A)|1\rangle_A|1\rangle_B.$$

By means of a local operation (a bit flip X_A) Alice can convert this state to

$$|1\rangle_A|0\rangle_B \pm |0\rangle_A|1\rangle_B,$$

apart from an irrelevant overall phase factor. The latter state can also directly be produced by either Alice or Bob by creating that state locally and subsequently using a *qubit*. Starting from an *ebit* as above, Bob, too, can apply local operations and produce

$$\exp(2i\phi_A)|1\rangle_A|0\rangle_B \pm \exp(2i\phi_B)|0\rangle_A|1\rangle_B.$$

Since all these entangled states are connected by local operations, these are all equivalent definitions of an *ebit*.

5. A *refbit* is, like an *ebit*, a shared resource between Alice and Bob. It is defined as Alice and Bob sharing a (product) state of the form

$$(|0\rangle_A + \exp(i\phi_A)|1\rangle_A)(|0\rangle_B + \exp(i\phi_A)|1\rangle_B),$$

or equivalently

$$(|0\rangle_A + \exp(i\phi_B)|1\rangle_A)(|0\rangle_B + \exp(i\phi_B)|1\rangle_B).$$

This definition is such that Alice can use a *qubit* to establish a *refbit*. Since neither Alice nor Bob are aware of any of the phases appearing in the definition of a *refbit*, they cannot establish a *refbit* by local means, in spite of it being a product state.

6. For later use, we also define a *refbit(2)*. Again, this is a shared resource between Alice and Bob. It is defined as Alice and Bob sharing a state of the form

$$(|00\rangle_A + \exp(2i\phi_A)|11\rangle_A)(|00\rangle_B + \exp(2i\phi_A)|11\rangle_B).$$

One can probabilistically generate a *refbit(2)* from 2 *refbits* (succeeding with 50% chance), but not the other way around.

In addition to the above resources, which do not use any coding, we can also define encoded versions of the same resources. In particular, Alice and Bob can communicate without sharing a reference frame using the encodings discussed in [2]. That paper actually discusses a slightly different situation where Alice and Bob do not even agree on the definitions of $|0\rangle$ and $|1\rangle$. In that case, which would correspond to the scenario of Alice and Bob using *massive* spin-1/2 particles to communicate, one needs 4 physical qubits to encode one logical qubit. On the other hand, within the present communication model, Alice and Bob can encode in the following reference-frame independent way, using just two physical qubits to encode one logical qubit. For example, they could use

$$\begin{aligned}|0\rangle_L &= |0\rangle|1\rangle,\\ |1\rangle_L &= |1\rangle|0\rangle.\end{aligned} \tag{4}$$

Alice can encode a logical qubit by performing

$$|0\rangle(a|0\rangle + b\exp(i\phi_A)|1\rangle) \mapsto \exp(i\phi_A)(a|0\rangle_L + b|1\rangle_L). \tag{5}$$

We denote resources that make use of this type of encoding by capitalizing the corresponding unit. So we have *Qubits*, *Cbits*, *Ebits*, and *Cobits*, but *Refbits* do not make any sense.

V. RELATIONS BETWEEN RESOURCES

With these definitions we can write down simple relations of the form $X \geq Y$, following [6], which mean that the resource X can be used to simulate resource Y (and $X = Y$ if and only if both $X \geq Y$ and $Y \geq X$).

We consider first coherent protocols, in which the environment, which appears in the definition of a *cbit*, plays no role. Subsequently, we consider incoherent protocols that (implicitly or explicitly) yield or use *cbits*.

A. Coherent protocols

With the above definitions it is straightforward to obtain protocols that achieve

$$\begin{aligned} 1\,qubit &\geq 1\,ebit, \\ 1\,qubit &\geq 1\,cobit, \\ 1\,cobit &\geq 1\,ebit, \\ 1\,qubit &\geq 1\,refbit, \\ 1\,qubit + 1\,ebit &\geq 1\,refbit(2). \end{aligned} \tag{6}$$

We now consider several slightly more complicated protocols that convert one type of resource into another.

1. Protocol C1

First, consider a protocol that is simpler than teleportation, yet achieves the same resource-wise. Alice is given a physical qubit in the state (possibly unknown to her) $a|0\rangle_A + b|1\rangle_A$. Using a *cobit*, she accomplishes

$$a|0\rangle_A + b|1\rangle_A \mapsto a|0\rangle_A|0\rangle_B + b\exp(i\phi_A)|1\rangle_A|1\rangle_B.$$

Then on her half of this state plus an ancilla in state $|0\rangle$ she performs the following 2-qubit operation

$$\begin{aligned} |0\rangle|+\rangle &\mapsto |0\rangle|+\rangle, \\ |0\rangle|-\rangle &\mapsto \exp(i\phi_A)|1\rangle|-\rangle, \end{aligned}$$

where $|\pm\rangle = |0\rangle \pm \exp(i\phi_A)|1\rangle$. This leads to the state

$$|0\rangle_{A1}|+\rangle_A(a|0\rangle_B + b|1\rangle_B) + \\ \exp(i\phi_A)|1\rangle_{A1}|-\rangle_A(a|0\rangle_B - b|1\rangle_B).$$

Subsequently, Alice uses another *cobit* to copy her ancilla $A1$ into an ancilla $B1$ at Bob's site. He then performs the operation

$$\begin{aligned} |0\rangle|1\rangle &\mapsto |0\rangle|1\rangle, \\ |1\rangle|1\rangle &\mapsto -|1\rangle|1\rangle, \end{aligned}$$

to end up with the state

$$(|0\rangle_{A1}|+\rangle_A|0\rangle_{B1} + \exp(i\phi_A)|1\rangle_{A1}|-\rangle_A|1\rangle_{B1}) \\ \otimes(a|0\rangle_B + b|1\rangle_B).$$

The first term can be converted into one *ebit* by Alice, the second term shows Alice has managed to simulate a *qubit*. Thus, this protocol achieves

$$2\,cobits \geq 1\,qubit + 1\,ebit. \tag{7}$$

First we note Alice and Bob do not have to share a reference frame or any *refbits* to achieve this. Second we note this relation holds without using a catalyst, thus slightly improving Eq. (4) in [6], which was derived there using an extra *ebit* on both sides of the relation.

2. Protocol C2

A similar protocol starts with Alice producing

$$a|0\rangle_A + b\exp(i\phi_A)|1\rangle_A.$$

Using a *cobit* Alice and Bob share the state

$$a|0\rangle_A|0\rangle_B + b\exp(2i\phi_A)|1\rangle_A|1\rangle_B.$$

Then Alice flips her physical qubit to get

$$a|1\rangle_A|0\rangle_B + b|0\rangle_A|1\rangle_B.$$

apart from an irrelevant overall phase factor $\exp(i\phi_A)$. Sending her physical qubit to Bob (and thus using one *qubit*) leaves him with an encoded *Qubit*. Thus, we find

$$1\,cobit + 1\,qubit \geq 1\,Qubit. \tag{8}$$

3. Protocol C3

By starting out with a *refbit*, $|0\rangle + \exp(i\phi_B)|1\rangle$, Alice can use a *cobit* to produce

$$|0\rangle_A|0\rangle_B + \exp(i\phi_A + i\phi_B)|1\rangle_A|1\rangle_B,$$

which by local transformations can be transformed into an *Ebit*. Hence

$$1\,cobit + 1\,refbit \geq 1\,Ebit. \tag{9}$$

Note that starting with just one *ebit*, Alice and Bob can generate by local operations the state

$$\exp(i\phi_A)|0\rangle_L|1\rangle_L + \exp(i\phi_B)|1\rangle_L|0\rangle_L$$

but that state contains both ϕ_A and ϕ_B, and so is not a reference-frame invariant state, and hence not an *Ebit*.

4. Protocol C4

Instead of using a *refbit* and a *cobit* to obtain an *Ebit*, it is easy to check that Alice and Bob could also start out with an *ebit* and then use a *cobit* to end up with an *Ebit*, thus leading to

$$1\,cobit + 1\,ebit \geq 1\,Ebit. \tag{10}$$

5. Superdense coding

Finally, consider the coherent version of superdense coding. Alice and Bob start with an *ebit*, say $|1\rangle_A|0\rangle_B + |0\rangle_A|1\rangle_B$. Alice, moreover, has two ancilla physical qubits in a state $|a_1\rangle|a_2\rangle$, where a_1 and a_2 take on the values 0 or 1. She then performs the following 3-qubit operation, conditioned on the state of the two ancilla's (the first two kets in the equations below)

$$\begin{aligned}
|1\rangle|0\rangle|0\rangle &\mapsto |1\rangle|0\rangle|0\rangle \\
|1\rangle|0\rangle|1\rangle &\mapsto |1\rangle|0\rangle|1\rangle \\
|0\rangle|1\rangle|0\rangle &\mapsto |0\rangle|1\rangle|0\rangle \\
|0\rangle|1\rangle|1\rangle &\mapsto -|0\rangle|1\rangle|1\rangle \\
|0\rangle|0\rangle|0\rangle &\mapsto \exp(i\phi_A)|0\rangle|0\rangle|1\rangle \\
|0\rangle|0\rangle|1\rangle &\mapsto \exp(-i\phi_A)|0\rangle|0\rangle|0\rangle \\
|1\rangle|1\rangle|0\rangle &\mapsto -\exp(i\phi_A)|1\rangle|1\rangle|1\rangle \\
|1\rangle|1\rangle|1\rangle &\mapsto \exp(-i\phi_A)|1\rangle|1\rangle|0\rangle
\end{aligned}$$

Subsequently, Alice uses one *qubit* to send the physical qubit A to Bob. In the four possible cases Alice and Bob end up with

$$|1\rangle|0\rangle \otimes (|1\rangle|0\rangle + |0\rangle|1\rangle)$$

$$|0\rangle|1\rangle \otimes (-|1\rangle|0\rangle + |0\rangle|1\rangle)$$

$$|0\rangle|0\rangle \otimes (\exp(-i\phi_A)|0\rangle|0\rangle + \exp(i\phi_A)|1\rangle|1\rangle)$$

$$|1\rangle|1\rangle \otimes (\exp(-i\phi_A)|0\rangle|0\rangle - \exp(i\phi_A)|1\rangle|1\rangle)$$

The last two entangled states are indistinguishable to Bob. More precisely, both are equal mixtures of $|0\rangle|0\rangle$ and $|1\rangle|1\rangle$ to him. One of the two classical bits a_1 and a_2, therefore, cannot be sent coherently without a reference frame, but the other bit can. Thus, by starting off her ancilla bits in only two possible states, corresponding to $|0\rangle_L$ or $|1\rangle_L$, Alice and Bob achieve

$$1\,qubit + 1\,ebit \geq 1\,Cobit. \tag{11}$$

6. Comparing encoded and unencoded resources

Performing superdense coding and protocol C1 with encoded resources immediately gives us

$$1\,Qubit + 1\,Ebit = 2\,Cobits. \tag{12}$$

These encoded resources can be obtained from unencoded resources, by the results obtained above. In particular, the left-hand side, a *Qubit* and an *Ebit*, can be obtained from 2 *cobits*, 1 *qubit*, and 1 *ebit*. The right-hand side can indeed be obtained from the same unencoded resources. Namely, the two *cobits* can be converted into 1 *qubit* and 1 *ebit*. Subsequently, 2 *qubits* and 2 *ebits* can be converted into 2 *Cobits*.

Obviously, we can also use 2 *cobits* directly to yield one *Cobit*. From this and Eqs (8) and (10) one sees that a *cobit* can always be used to convert an unencoded resource, a *qubit*, an *ebit*, and a *cobit*, into the corresponding encoded form.

We also note that unencoded resources cannot be obtained from just encoded resources. The reason is simply that unencoded resources contain formation about Alice's and Bob's local reference frames, while encoded resources do not (which is the whole point of encoding).

B. Incoherent protocols

1. Superdense coding

Returning to superdense coding, we note that Alice could decide to start off her ancilla bits in only three possible initial states, 01, 10 or 00, with equal probabilities. In the incoherent version she thus succeeds in sending $\log_2(3)$ classical bits to Bob, rather than 2 when they share a reference frame. Moreover, in the case that Alice chose 00, Bob actually ends up with a state in his possession that still contains the phase ϕ_A, $|00\rangle + \exp(2i\phi_A)|11\rangle$. Clearly, this can be converted into a *refbit(2)*. Thus, Alice and Bob actually achieve

$$1\,qubit + 1\,ebit \geq \log_2(3)\,cbits + 1/3\,refbit(2). \tag{13}$$

Now, with one *refbit* Bob cannot get more *cbits* out of this protocol, basically since he has to compensate for extra phases of $2\phi_A$ appearing. But with two *refbits* he can do a better job of decoding in the classical case, and, moreover, can sometimes save his *refbits*. In particular, Bob has a probability $P = 1/4$ to unambiguously discriminate between the two states

$$(|00\rangle \pm \exp(2i\phi_A)|11\rangle) \otimes (|0\rangle + \exp(i\phi_A)|1\rangle)^{\otimes 2}.$$

(There are two ways of obtaining the probability $P = 1/4$: either we write down mixtures over the unknown phase ϕ_A for the two possible states and calculate the unambiguous-state discrimination probability for two mixed states, or we let Bob project onto subspaces with equal phase factors $\exp(in\phi_A)$, where $n = 0, 1, 2, 3, 4$, and subsequently let him perform unambiguous state discrimination between the projections of the two states within those subspaces.) Hence, if Alice chooses her two classical bits as either 01 or 10 with probability $p/2$ each, and as 00 or 11 with probability $(1-p)/2$ each, then they achieve

$$\begin{aligned} &1\,qubit + 1\,ebit + 2\,refbits \geq \\ &(H(p) + (1+3p)/4)\,cbits + 2p\,refbits, \end{aligned} \tag{14}$$

with $H(p)$ the Shannon entropy $H(p) = -p\log_2 p - (1-p)\log_2(1-p)$. Note that in this case no further resources are left over, in particular, there is no *refbit(2)* at the end of the protocol. Choosing $p = 2/3$ we gain 1/12 of a *cbit* compared to (13) while using up 2/3 *refbits*:

$$\begin{aligned} &1\,qubit + 1\,ebit + 2\,refbits \geq \\ &(\log_2 3 + 1/12)\,cbits + 4/3\,refbits. \end{aligned} \tag{15}$$

The amount of communicated *cbits* using two *refbits* is maximized to 1.6732 *cbits* achieved for $p = p_0 \approx 0.627$.

Instead of using two *refbits*, it is better for Bob to use one *refbit(2)*. It is easy to verify that Bob now can succeed in unambiguously distinguishing the two states

$$(|00\rangle \pm \exp(2i\phi_A)|11\rangle) \otimes (|00\rangle + \exp(2i\phi_A))|11\rangle$$

with probability $P = 1/2$. This then yields

$$\begin{aligned} 1\, qubit + 1\, ebit + 1\, refbit(2) \geq \\ (H(p) + (p+1)/2)\, cbits + p\, refbits(2). \end{aligned} \tag{16}$$

We can also calculate what Alice and Bob can gain from sharing many *refbits*. The important determining factor here is the probability P_N for Bob to unambiguously discriminate between the states

$$(|00\rangle \pm \exp(2i\phi_A)|11\rangle) \otimes (|0\rangle + \exp(i\phi_A)|1\rangle)^{\otimes N},$$

when Alice and Bob share N refbits. It is straightforward to find for even values of N

$$1 - P_N = \frac{\begin{pmatrix} N \\ N/2 \end{pmatrix} + \begin{pmatrix} N \\ N/2+1 \end{pmatrix}}{2^N} \tag{17}$$

while for odd values of N one finds the same result as for $N-1$. That is, a single extra *refbit* never helps to improve upon the case with an even number of *refbits*. So we find that P_N approaches unity only slowly. Asymptotically one has

$$P_N \approx 1 - \frac{4}{\sqrt{2\pi N}}.$$

In terms of P_N and p, superdense coding leads to the following trade-off relation

$$\begin{aligned} 1\, qubit + 1\, ebit + N\, refbits \geq \\ (H(p) + (1 - P_N)p + P_N)\, cbits + pN\, refbits. \end{aligned} \tag{18}$$

As expected, in the limit of $N \to \infty$ one recovers standard superdense coding in the presence of a shared reference frame: in particular, one uses $p = 1/2$ to send 2 *cbits*, and one saves half of the *refbits*.

2. Teleportation

The coherent version of teleporation works only if Alice and Bob share a reference frame or use phase-invariant encoding. However, it is still interesting to consider the resources needed for the incoherent (standard) version of teleportation. Without a reference frame teleportation only succeeds for two out of four outcomes of Alice's Bell measurement, thus leading to

$$2\, cbits + 1\, ebit \geq 1/2\, qubit. \tag{19}$$

Here we are interested only in perfect fidelity teleportation, and in only half of the cases do they succeed in this endeavor (and they know when they succeed and when not). When Alice and Bob share *refbits*, the probability to succeed in perfect teleportation increases. Namely, in the cases where Alice gets a "wrong" measurement outcome, Bob can still try to project onto the correct subspace. The probability to succeed turns out to be the same probability P_N as we encountered before when we considered superdense coding. Thus we find the duality between the two protocols persists in the absence of a reference frame and sharing an arbitrary number of *refbits*. Here we get (for even numbers of *refbits*)

$$2\, cbits + 1\, ebit + 2N\, refbits \geq (P_{2N}+1)/2\, qubit + N\, refbits. \tag{20}$$

For example, with 2 *refbits* one succeeds in perfect teleportation with probability 5/8, but, as before, when using a *refbit(2)*, the chances increase, and one gets

$$2\, cbits + 1\, ebit + 1\, refbit(2) \geq 3/4\, qubit + 1/2\, refbit(2). \tag{21}$$

In the limit $N \to \infty$ one recovers the results for teleportation in the presence of a shared reference frame, and again one saves half of the *refbits*.

3. Converting ebits to Ebits

In this subsection we consider some more protocols that convert unencoded into encoded resources. These protocols in fact use the present formalism to reformulate and unify results obtained before in Refs. [3] and [7]. Starting out with 2 *ebits*, $(|0\rangle|1\rangle + |1\rangle|0\rangle)^{\otimes 2}$, Bob can perform a projective measurement onto subspaces with even or odd numbers of $|1\rangle$ appearing in his two-qubit space. This leads with probability 1/2 to an *Ebit*, and with probability 1/2 to a state that one would normally called entangled, but which is not equivalent to an *Ebit*. Thus, we get

$$2\, ebits \geq 1/2\, Ebit. \tag{22}$$

This relation in fact reexpresses the statement of Eq. (5) in the second paper of Ref. [7], namely, that the amount of entanglement E_P, for 2 *ebits* is 1/2, although it is zero for 1 *ebit*. We can achieve the same conversion with a *refbit*:

$$1\, ebit + 1\, refbit \geq 1/2\, Ebit. \tag{23}$$

Thus for the purpose of extracting "useful" entanglement out of an *ebit*, another *ebit* or a *refbit* achieve the same. Both relations also express how data hiding works in the presence of superselection rules. Namely, an *ebit* can be used to hide one classical bit, by encoding it in one of two states $|0\rangle_A|1\rangle_B \pm |1\rangle_A|0\rangle_B$. However, neither Alice nor Bob can locally distinguish these two states at all. But by using either a *refbit* or a second *ebit*, they can convert it with 50% probability to one of two different forms of an *Ebit*. Since the latter is in encoded form, the classical bit can be retrieved.

We might as well remark here that although *refbits* and *ebits* are similar for certain purposes (see, for example, [3]), they are definitely not the same. In particular, a *refbit* cannot be converted into an *ebit* by local operations and classical communication, but one can achieve the converse by remote state preparation,

$$1\,ebit + 1\,cbit \geq 1\,refbit. \tag{24}$$

Also, whereas an *ebit* can be converted into a secret shared random classical bit, a *refbit* cannot.

Alice and Bob can reach the optimum conversion of 1 *ebit* to 1 *Ebit* in the limit of infinitely many *refbits*. Bob projects onto subspaces with a fixed number of states $|1\rangle$ on his $(N+1)$ physical qubits (one for the *ebit*, the others from the N *refbits* he shares with Alice). The outcomes do not always lead to maximally entangled encoded states, but they do always lead to encoded states. The average entanglement they gain with 2 *refbits*, for example, is

$$1\,ebit + 2\,refbits \geq (3\log_2(3)/4 - 1/2)\,Ebit. \tag{25}$$

By using a large number N of *refbits*, they approach a full *Ebit*, according to

$$1\,ebit + N\,refbits \geq (1 - 1/(2N))\,Ebit. \tag{26}$$

C. Asymptotic relations

So far we only considered single-shot protocols, in which a single use of certain resources is analyzed, but one may also be interested in the results that can be obtained with many uses of a given resource. For example, let us consider incoherent superdense coding. Without *refbits*, Alice and Bob in a single-shot protocol can achieve

$$1\,qubit + 1\,ebit \geq \log_2(3)\,cbits + 1/3\,refbit(2). \tag{27}$$

They achieve this if Alice applies one of three operations to her physical qubit, I, Z, X_A. But if they use 2 *qubits* and 2 *ebits* the same protocol can yield slightly more than twice the right-hand side. For instance, suppose Alice still applies one of the same three operations I, Z, X_A on the first physical qubit, with probability 1/3 each. On her second physical qubit, she also applies I or Z with probability 1/3 each, but she applies now either X_A or Y_A with probability 1/6 each. Now the combination $X_A^{(1)}X_A^{(2)}$ can be unambiguously distinguished by Bob from $X_A^{(1)}Y_A^{(2)}$ with probability P=1/2. Thus, they gain 1/18th of a classical bit, but end up with only 2/9th of a *refbit(2)*. Thus

$$2\,qubits + 2\,ebits \geq (\log_2(3) + \frac{1}{18})\,cbits + 2/9\,refbit(2). \tag{28}$$

The protocol above is just to illustrate that Alice and Bob can gain classical bits, it is not optimized for anything in particular. It does illustrate how precious Hilbert space is wasted. It is much better indeed to extend the phase-reference-invariant encoding used above to higher dimensions. It is trivial to accomplish this: for a fixed number N of physical qubits we choose states with some fixed number N_1 of 1s, where $N_1 \approx [N/2]$. The dimension of the subspace spanned by states of that form is $N!/(N1!(N-N1)!)$. For large N this number approaches

$$\frac{N!}{N1!(N-N1)!} \approx \frac{2^N}{\sqrt{\pi N/2}}.$$

That means we can encode $N - \log_2(\pi N/2)$ encoded *Qubits* into N *qubits*. Asymptotically, therefore, we will have

$$1\,qubit \geq 1\,Qubit\ \ (a), \tag{29}$$

with (a) denoting the relation holds asymptotically for many copies of the resources. Similarly, suppose Alice and Bob start out with a large number N of *ebits*. Alice and Bob can do a projective measurement on subspaces spanned by states with a fixed number of 1s. Both will find with high probability a subspace with about $[N/2]$ 1s. Thus, they end up with high probability (approaching unity) $N - \log_2(\pi N/2)$ *Ebits*. Thus,

$$1\,ebit \geq 1\,Ebit\ \ (a). \tag{30}$$

This relation in fact reexpresses a fact analyzed in [3]. As a result, superdense coding leads to

$$1\,qubit + 1\,ebit \geq 2\,cbits\ \ (a). \tag{31}$$

VI. SUMMARY AND DISCUSSION

We presented a formalism for describing resources in quantum communication that extends that of Ref. [6] to allow for the absence of shared reference frames. It naturally leads to the definition of a new resource, the *refbit*, and to modifications of the definitions of known resources, such as the *ebit* and the *cobit*.

The formalism can be used to describe both known theoretical results and practical experiments. For example, the relation

$$2\,ebits \geq 1/2\,Ebit \tag{32}$$

has the same meaning as the statement in [7] that the entanglement E_P in two copies of the state $|0\rangle|1\rangle + |1\rangle|0\rangle$ is 1/2. That is, in the presence of a $U(1)$-superselection rule one needs two copies of that state in order to generate *accessible* entanglement with probability 1/2. It in fact also expresses the fact that quantum data hiding in the presence of superselection rules [3] allows one to hide one classical bit of information in an *ebit*, which can be unlocked with probability 1/2 if another *ebit* is used as a resource.

To give a practical example described by our formalism, consider today's quantum key distribution protocols. Probably the best method to encode quantum information is in the relative phase of weak coherent states. That is, in the standard implementation of the BB84 protocol Alice sends Bob one of four states

$$|\alpha \exp(i\phi_A)\rangle|\alpha \exp(i(\phi_A + \phi_k))\rangle \; k = 1 \ldots 4, \tag{33}$$

where $\phi_k = k\pi/2$. Here $|\alpha\rangle$ denotes a coherent state with amplitude α, where typically $|\alpha|^2 \approx 0.1$. Even if polarization is used to encode information in weak coherent states, one can still rewrite the states used in the form (33) [10]. Clearly, the information is encoded in a way that does not depend on the value of ϕ_A. In other words, this is a phase-reference independent way of encoding, and one could say that the BB84 protocol makes use of *Qubits*.

On the other hand, one could imagine the state $|\alpha \exp(i\phi_A)\rangle$ shared in advance between Alice and Bob, and in that case this is akin to sharing a *refbit*. It is not quite the same, as to lowest order in $|\alpha|$ the shared state is $|0\rangle + \alpha \exp(i\phi_A)|1\rangle$, rather than an equal superposition of $|0\rangle$ and $\exp(i\phi_A)|1\rangle$.

Similarly, the B92 protocol would have Alice send states to Bob of the form

$$|\beta \exp(i\phi_A)\rangle|\alpha \exp(i(\phi_A + \phi_k))\rangle \; k = 1, 2, \tag{34}$$

where $|\beta| \gg |\alpha|$ and there are only two phases chosen by Alice. The idea is indeed to provide Bob with a full phase reference to allow him to unambiguously distinguish the two possible states with a reasonable (but not too large!) probability. This method is more akin to sharing N *refbits*, with N large. That method is wasteful in terms of resources (for other purposes it would be better to use *Qubits* or an encoding like that of Ref. [2]) but the large reference pulse is necessary for security purposes. As an aside we note that creating superpositions of different coherent states (even weak ones) is very complicated in practice, so that sending physical qubits this way is far from trivial.

For another practical example, we return (hopefully for the last time) to the discussions about teleportation with continuous variables (for details, see Refs. [11]). In the language of the present paper, what the typical teleportation experiment does is just to use many *refbits* to enable certain operations. For example, Bob's unitary operation at the end of the teleportation protocol must contain a phase ϕ_A, as it has been introduced by Alice's joint measurement. In this same context, it was concluded in [11] that a certain mixture of two-mode squeezed states in combination with a large phase reference pulse does possess distillable entanglement, whereas the mixture without phase reference contains no entanglement. In the language of our formalism, a two-mode squeezed state by itself contains only *ebits*, but *refbits* in the form of a laser acting as a phase reference can be used to generate *Ebits*. Indeed, the procedure used to distill the entanglement is essentially the same as that used to convert an *ebit*, in a single-shot protocol, to an *Ebit* by using a *refbit*.

Also, we have shown that (incoherent) teleportation, in the single-shot version, succeeds with probability approaching unity only if one shares a large number of *refbits*. This then qualifies and quantifies the statement in [12] that in a teleportation protocol one always needs to share a reference frame of some sort.

To return to more abstract concepts, we have shown that the *cobit*, as introduced in [6], becomes a more powerful resource (relative to other resources) when no phase reference is shared. First of all, a *cobit* can always be used to convert an unencoded resource into the encoded equivalent, such as an *ebit* to an *Ebit*, or a *qubit* to a *Qubit*. Second, with a reference frame present one has the equality

$$2\, cobits = 1\, qubit + 1\, ebit \;\; (*), \tag{35}$$

with the * indicating this equality holds when a phase reference is shared. In contrast, without shared phase reference we do have

$$2\, cobits \geq 1\, qubit + 1\, ebit, \tag{36}$$

but only

$$1\, qubit + 1\, ebit \geq 1\, Cobit. \tag{37}$$

These relations show that the value of a *cobit* is exactly in between that of a *qubit* and an *ebit* when there is a shared phase reference, but that it moves closer to a *qubit* the less of a shared phase reference one has. The reason for a *cobit* to move closer to a *qubit* is that it can be implemented only by sending a physical qubit. Being able to actually send a physical qubit becomes more important in the absence of a reference frame, since one obviously needs to send something in order to establish a reference frame.

Let us return to the incoherent version of superdense coding. With N large we found the relation

$$1\, qubit + 1\, ebit + N\, refbits \geq (2 - 1/\sqrt{\pi N})\, cbits. \tag{38}$$

This follows from relation (18) by substituting $p = 1/2$ and replacing $N \to 2N$ and using N refbits catalytically. We note that Alice and Bob could alternatively use N *refbits* to estimate the phase difference $\phi_A - \phi_B$. Subsequently, Bob could then decode Alice's message by using his best estimate of the alignment of Alice's reference frame. That would transfer with high probability 2 classical bits from Alice to Bob as well in a superdense coding protocol. The difference between the two approaches is that in one case they get sometimes only 1 classical bit, but they know the bits are always correct; in the other case they always get 2 classical bits, but 1 bit might be incorrect and they do not know when.

Note, by the way, that using *refbits* to estimate the angle $\phi_A - \phi_B$ is the 2-D equivalent of the problem of estimating the Euler angles of a 3-D Cartesian system by using spin-1/2 systems [1]. But in the 2-D case, unlike in the 3-D case, anti-parallel spins do not perform any better than parallel spins, as there is an agreed-upon rotation axis that can be used to convert parallel spins into anti-parallel spins.

Finally, we considered the difference between single-shot protocols and asymptotic versions of the same protocols. In particular, encoding becomes a powerful tool in the asymptotic limit. For instance, whereas one requires an extra *cobit* in order to convert an *ebit* or a *qubit* into an encoded *Ebit* or *Qubit* in a single-shot protocol, asymptotically one needs no extra resources to achieve the same conversion. That is the same conclusion as reached in Ref. [2], of course. Note, though, that experiments in quantum communication typically do not implement the asymptotic version of protocols, but rather many instances of single-shot protocols.

---

[1] S. Massar and S. Popescu, Phys. Rev. Lett. **74**, 1259 (1995); N. Gisin and S. Popescu, *ibidem* **83**, 432 (1999); T. Rudolph, `quant-ph/9904037`; A. Peres and P. Scudo, *ibidem* **86**, 4160 (2001); **87**, 167901 (2001); E. Bagan, M. Baig, and R. Mũnoz-Tapia, *ibidem* **87**, 257903 (2001); T. Rudolph and L. Grover, *ibidem* **91**, 217905 (2003).

[2] S.D. Bartlett, T. Rudolph, and R.W. Spekkens, Phys. Rev. Lett. **91**, 027901 (2003).

[3] F. Verstraete, and J.I. Cirac, Phys. Rev. Lett. **91**, 010404 (2003); N. Schuch, F. Verstraete, and J.I. Cirac, Phys. Rev. Lett. **92**, 087904 (2004).

[4] A. Kitaev, D. Mayers, and J. Preskill, Phys. Rev. A **69**, 052326 (2004).

[5] S.D. Bartlett, T. Rudolph, and R.W. Spekkens, Phys. Rev. A **70**, 032307 (2004).

[6] A. Harrow, Phys. Rev. Lett. **92**, 097902 (2004).

[7] H. Wiseman and J.A. Vaccaro, Phys. Rev. Lett. **91**, 097902; J.A. Vaccaro, F. Anselmi, and H. Wiseman, `quant-ph/0311028`.

[8] S.J. van Enk and T. Rudolph, `quant-ph/0303096`.

[9] F. Spedalieri, `quant-ph/0409057`.

[10] M. Dusek, M. Jahma, and N. Lütkenhaus, Phys. Rev. A **62**, 022306 (2000).

[11] A. Furusawa *et al.*, Science **282**, 706 (1998); T. Rudolph and B.C. Sanders, Phys. Rev. Lett. **87**, 077903 (2001). S.J. van Enk and C.A. Fuchs, Phys. Rev. Lett. **88**, 027902 (2002); Quant. Inf. Comp. **2**, 151 (2002).

[12] S.J. van Enk, J. Mod. Optics **48**, 2049 (2001).

[13] The assumption here is, of course, that particular modes can be defined unambiguously without sharing a reference frame: for that purpose, too, we can use circular polarization, or the modes with cylindricially symmetric transverse mode profiles discussed in [9].

[14] In both implementations Alice and Bob do need to share something, namely knowledge of what they mean by "0" and "1", or by "left" and "right". That resource, though, seems sufficiently mild to allow it without further consideration

[15] Presumably, the superselection rule would apply only in the context of using different number states, not in the case of using different polarizations.