How to hide a secret direction

To cite this article: E Bagan et al 2007 New J. Phys. 9 244

View the article online for updates and enhancements.

Related content

- Beating noise with abstention in state estimation
  Bernat Gendra, Elio Ronco-Bonvehi, John Calsamiglia et al.

- Quantum communication using a bounded-size quantum reference frame
  Stephen D Bartlett, Terry Rudolph, Robert W Spekkens et al.

- Units of rotational information
  Yuxiang Yang, Giulio Chiribella and Qinheping Hu
How to hide a secret direction

E Bagan¹, J Calsamiglia¹,³, R Demkowicz-Dobrzański² and R Munoz-Tapia¹

¹ Grup de Física Teòrica and Institut de Física d’Altes Energies, Universitat Autònoma de Barcelona, Bellaterra 08193, Spain
² Center for Theoretical Physics, Polish Academy of Sciences, Warsaw, Poland
E-mail: john.calsamiglia@uab.es

New Journal of Physics 9 (2007) 244
Received 26 March 2007
Published 1 August 2007
Online at http://www.njp.org/
doi:10.1088/1367-2630/9/8/244

Abstract. We present a procedure that uses a multipartite quantum state to communicate a secret spatial direction when there is no shared reference frame between the preparer and the group of recipients. The procedure guarantees that the recipients can determine the direction if they perform joint measurements on the state, but fail to do so if they restrict themselves to local operations and classical communication (LOCC). We calculate the fidelity for joint measurements, give bounds on the fidelity achievable by LOCC, and prove that there is a non-vanishing gap between the two of them, even in the limit of infinitely many copies. The robustness of the procedure under particle loss is also studied. Additionally, we find bounds on the probability of discriminating by LOCC between the invariant subspaces of total angular momentum \( N/2 \) and \( N/2 - 1 \) in a system of \( N \) elementary spins.

³ Author to whom any correspondence should be addressed.
1. Introduction

A good number of quantum information protocols that take advantage of the laws of quantum mechanics to keep secrets in different scenarios have been put forward over recent years. Quantum key distribution [1], which is probably the most prominent example, allows two parties to establish a secret random key. Using quantum secret sharing protocols [2] one can share secret information (classical or quantum) among several parties, so that the so-called authorized set can perfectly unveil it whereas any other set of parties cannot to any extent. Finally, quantum data hiding [3] also allows for the possibility of sharing information (classical or quantum) among many parties, but with the promise that they can only unveil it by performing joint operations, i.e. any local strategy assisted with classical communication will reveal (almost) nothing.

Here, we present a procedure that uses spin-1/2 particles to share a secret direction in a similar fashion: the parties can unveil it only if they perform joint measurements on all particles. Three observations are in order here. Firstly, the estimation of the direction will always be limited by the quantum nature of measurements, and thus a perfect estimation of the secret direction is only possible in the limit of an infinite number of particles. Secondly, as in quantum data hiding, and in contrast to quantum secret sharing, the information that can be obtained by local operations and classical communications (LOCC), although negligible, is not strictly zero. Lastly, the information shared in quantum data hiding or secret sharing is abstract in the sense that it can be represented in terms of qubits or bits disregarding their particular physical support. In contrast, a direction contains information of a very particular sort: it is physical information. A direction is an intrinsic property of some physical systems. Similarly, codifying a particular direction on an N-body state $\rho$ in the absence of a reference frame involves a very specific operation, namely a rigid rotation $U^\otimes N \rho U^+_{\otimes N}$ (see e.g. work on establishing common reference frames [4]). Hence, protocols for direction sharing are distinct to those of quantum data hiding for which there are no constraints on how the information is encoded. In this paper we envision a scenario where the group of recipients do have a common reference frame (in contrast to the situation assumed in [5]), but no such frame is shared with the sender.

In the implementation of many quantum communication protocols it is implicitly assumed that the parties involved have a common reference frame. Depending on the choice of the degrees of freedom that encode the quantum information, the lack of a common reference frame can effect more (or less) the performance of a communication protocol (see [6] for a recent review on reference frames in quantum information). No matter what this choice is, a common reference...
frame of some sort is usually necessary (see however [7]). In tasks for which a spatial reference frame is required, quantum direction sharing could be a primitive to establish such common frames without compromising the security requirements of the communication protocol.

A central ingredient, and a shared motivation, to this work is quantum state estimation. The topics of quantum state estimation and discrimination [8] are arguably among the first quantum information theoretical problems with an important impact on other research areas in quantum information ranging from entanglement theory [9], to state disturbance and teleportation [10] or quantum cloning [11]. Also, very recently Bacon et al [12] have found new efficient quantum algorithms by recasting some computational problems in terms of state estimation.

The usual scenario in state estimation is to consider \( N \) copies of a given unknown state and study the performance of different protocols (according to some figure of merit) as a function of \( N \). The action of general unitaries on qubits is the same as that of the physical rotations on spin-1/2 systems. Hence, all the results regarding the fidelity of a state estimation protocol under collective, local fixed and local adaptive measurements can be applied in the context of direction estimation. A common conclusion from these results is that all protocols achieve perfect determination in the limit of infinite number of copies, i.e. the fidelity (see below for a precise definition) is \( F = 1 - \mathcal{O}(N^{-1}) \). In this paper, we build on recent work [13], where the effect of correlations on the fidelity of permutation-invariant states is calculated and its relation to universal cloning machines is discussed. We provide exact results for joint measurements and non-trivial bounds for LOCC measurements. We find the surprising result that for local protocols the fidelity does not reach its optimal value (\( F = 1 \)) even when an infinite number of copies is available. However, when joint measurements are used, the very same state provides the fidelity of a perfect ‘gyroscope’, i.e. \( N \) spins pointing in the same direction\(^4\).

In order to illustrate the direction hiding protocol, we imagine the following fictitious scenario: a space station sends its (large) corps of space explorers to look for resources in other galaxies. The official in charge of the operation wants to make sure that the whole corps sticks together. To this end, he provides every explorer with a single spin-1/2 particle, and with a set of instructions that specify how to obtain the direction home, which has been encoded in the quantum state of the spins. Upholding the principle of equality, the preparer applies a random permutation on the state of her choice before delivering it to the explorers. The average fidelity obtained in this way is exactly the same as if she had started off with a permutation invariant state. The essential property of the state is that only by performing joint measurements on it, one can retrieve the direction home with accuracy, thus forcing the corps to stick together. If a significant fraction of it is left behind or refuses to join the rest, then the corps will not be able to make it back home. At the same time if a small fraction is captured by unfriendly forces, the rest of the corps will still be able to decode the direction faithfully, while the enemy will not be able to learn the whereabouts of the space station.

2. Direction hiding state

Here, we give an \( N \)-spin state that encodes the unknown direction, denoted with the unit Bloch vector \( \vec{n} \), in such a way that it can be estimated perfectly by joint measurements, but extremely poorly by LOCC measurements. We use the fidelity \( F \) as a figure of merit to quantify the explorers’

\(^4\) We note in passing that there are non-permutation invariant \( N \)-partite states for which \( F = 1 - \mathcal{O}(N^{-2}) \), as shown in [14].
ability to determine the direction, $F = \langle f \rangle \equiv (1 + \Delta)/2$ with $f = (1 + \vec{n} \cdot \vec{s}_\chi)/2 \equiv (1 + \Delta_{n, \chi})/2$, where $\vec{s}_\chi$ is their guess for $\vec{n}$ based upon the measurement outcome $\chi$. The average is taken over all possible directions and over all outcomes.

An arbitrary permutation invariant state can be written as [15], (we assume $N$ is even for simplicity)

$$\rho = \sum_{j=0}^{N/2} \sum_{\alpha=1}^{n_j} \rho_{(j,\alpha)} \quad \text{with} \quad \rho_{(j,\alpha)} = \sum_{m,m'=\pm j} \lambda_{mm'}^{(j)} |j, m, \alpha\rangle \langle j, m', \alpha|,$$

where $J = N/2$, $j$ is the total angular momentum, $m$ is its projection along the $\vec{z}$ axis, and $n_j$ is the multiplicity of the spin-$j$ representation. Given a generalized measurement, represented by a positive operator-valued measure (POVM) $\mathcal{M} = \{M_\chi\}$, the expected fidelity can be written as,

$$\Delta = \sum_\chi \int d\vec{n} \vec{s}_\chi \cdot \vec{n} \ Tr \left[ M_\chi \rho(\vec{n}) \right],$$

where $\rho(\vec{n}) = U(\vec{n}) \rho(\vec{z}) U^\dagger(\vec{n})$, $\sum$ represents the sum over a continuous and/or discrete set of POVM elements, and $dn$ is the standard measure on the 2-sphere normalized so that $\int dn = 1$, i.e., in spherical coordinates $dn = d\Omega/(4\pi) = d(cos \theta) d\phi/(4\pi)$. The rotation $U(\vec{n})$ by definition takes the unit vector $\vec{z}$ into $\vec{n}$; i.e., it is a representation of the three-dimensional rotation $R(\vec{n})$, where $\vec{n} = R(\vec{z}) \vec{z}$. We see that

$$\Delta = \sum_\chi \int d\vec{n} \vec{s}_\chi \cdot \vec{n} \ Tr \left[ R^{-1}(\vec{s}_\chi) \vec{n} \right] W \left[ M_\chi \rho(\vec{n}) \right].$$

Defining $\vec{n}' = R^{-1}(\vec{s}_\chi) \vec{n}$, we have $R(\vec{n}') = R^{-1}(\vec{s}_\chi) R(\vec{n})$, and thus

$$\rho(\vec{n}) = U(\vec{n}) \rho(\vec{z}) U^\dagger(\vec{n}) = U(\vec{n}) U(\vec{n}') \rho(\vec{n}') U^\dagger(\vec{n}) = U(\vec{s}_\chi) \rho(\vec{n}') U^\dagger(\vec{s}_\chi).$$

Substituting in (1) we have

$$\Delta = \int d\vec{n} \vec{s}_\chi \cdot \vec{n} \ Tr \left[ \Omega \rho(\vec{n}) \right], \quad \text{with} \quad \Omega = \sum_\chi U^\dagger(\vec{s}_\chi) \rho(\vec{s}_\chi) U(\vec{s}_\chi).$$

We now recall that $\vec{z} \cdot \vec{n} = \cos \theta = \mathcal{D}^{(1)}_{00}(\vec{n})$, where $\mathcal{D}^{(j)}_{mm'}(\vec{n}) = \langle jm\gamma| U(\vec{n}) | jm'\alpha\rangle$ are the rotation matrices [16]. By writing (2) in the basis $\{|j, m, \alpha\rangle\}$ we obtain

$$\Delta = \sum_{j,\alpha} \sum_{m,m'} \int d\vec{n} \mathcal{D}^{(j,\alpha)}_{mm'} \mathcal{D}^{(1)}_{00}(\vec{n}) \mathcal{D}^{(j,\alpha)}_{m'm}(\vec{n}) \mathcal{D}^{(j,\gamma)}_{mm'}(\vec{n}),$$

where we have used the notation $\mathcal{D}^{(j,\alpha)}_{mm'} = \langle jm\alpha| O | jm'\alpha\rangle$ for the matrix elements of an operator $O$. Using the orthogonality relations [16] of the rotation matrices we can perform the integral over $dn$ and cast (3) as [15]

$$\Delta = \sum_{j,\alpha} \sum_{m,m'} \mathcal{D}^{(j,\alpha)}_{mm'} \mathcal{D}^{(j,\alpha)}_{m'm}(\vec{n}) \mathcal{D}^{(j,\gamma)}_{mm'}(\vec{n}) = \sum_{j} n_j \left( \sum_{m} m \lambda_{mm'}^{(j)} \right) \left( \sum_{m} m \frac{\Omega_{mm'}^{(j)}}{j(j+1)(2j+1)} \right).$$

New Journal of Physics 9 (2007) 244 (http://www.njp.org/)
The completeness of the POVM implies \( \sum_m \Omega_m^{(j)}/(2j+1) = 1 \). From here it follows that the optimal fidelity is given by

\[
\Delta = \sum_j \frac{n_j}{j+1} \left| \sum_m m \lambda_m^{(j)} \right|.
\]  

(5)

For a fixed single-particle purity \( r \) (i.e. \( \rho_1 = (1 + r \vec{n} \cdot \vec{\sigma})/2 \), where \( \vec{\sigma} \) is a vector made out of the three Pauli matrices), this expression is maximized by

\[
\lambda_m^{(j)} = p \delta_{jm}; \quad \lambda_{m}^{(j-1)} = \frac{1-p}{N-1} \delta_{j-1,m}; \quad \lambda_m^{(j)} = 0, \quad \text{if } j < J - 1.
\]  

(6)

This can be easily seen by noticing that in order to reach the highest value of \( \Delta \) in (5) it is favorable to distribute the weights \( \lambda_m^{(j)} \) around the highest \( j \) and \( |m| \) values allowed by the constrains \( \sum_j n_j \lambda_m^{(j)} = 1 \) and \( r = (2/N) \langle J_z \rangle = \sum_j n_j m \lambda_m^{(j)} = 0 \). The obvious solution is to put all the weight in the two highest values of the angular momentum \( j = J \) and \( J - 1 \), and magnetic numbers \( m = J \) and \( m = -J + 1 \), respectively. The optimal state is thus

\[
\rho = p[J, J]_n + \frac{1-p}{N-1} \sum_{\alpha=1}^{N-1} [J - 1, -J + 1, \alpha]_n
\]

\[
= p |\vec{n}\rangle\langle\vec{n}|^\otimes N + \frac{1-p}{N} \sum_\sigma |\vec{n}\rangle\langle-\vec{n}|^\otimes N^{-2} |\psi^+\rangle\langle\psi^-|,
\]  

(7)

where we have introduced the notation \([j, m, \alpha]_n = U(\vec{s}) |jma\rangle|jma\rangle U(\vec{s})^\dagger\), \(|\vec{n}\rangle = U(\vec{n}) |\frac{1}{2} \frac{1}{2}\rangle\), and the sum in the second line is taken over all the \( N_\sigma \) permutations of the position of the singlet \( |\psi^-\rangle \), and where the value of \( p \) determines the purity of the local state through the relation \( p = [N(1 + r)/2 - 1]/(N - 1) \). In particular, one can take \( p = (N - 2)/(2N - 2) \) so that every individual spin is maximally mixed \( (r = 0) \) and contains no information about the direction. In spite of that, the parties can collectively estimate \( \vec{n} \) with a fidelity

\[
\Delta = p \frac{N}{N+2} + (1-p) \frac{N-2}{N} \approx 1 - \frac{2}{N}.
\]  

(8)

A measurement that attains this bound is given by the POVM elements

\[
M(\vec{s}, J) = (2J + 1) [J, J]_n, \quad M(\vec{s}, J - 1) = \frac{2J-1}{N-1} \sum_\alpha [J - 1, -J + 1, \alpha],
\]

which are now labeled by \( j = J, J - 1 \) and the continuous parameter \( \vec{s} \), i.e. it consists of two outcomes \( (j = J, J - 1) \) projection followed by the standard optimal direction-estimation measurement. The direction hiding state (7) encodes \( \vec{n} \) as efficiently as \( N \) parallel spins, i.e. yields the same fidelity for large \( N \). We recall that for \( N \) parallel spins \([17]\) \( \Delta = N/(N+2) \rightarrow 1 - 2/N \). In the following, we will prove that one can only reach this maximum fidelity under joint measurements, i.e. that for any LOCC strategy the fidelity does not reach one even in the strict limit \( N \rightarrow \infty \). This means that, no matter how large \( N \) is, if the space explorers do not perform collective measurements, with high probability they will not be able to return home. We note in passing that the proposed state and measurement scheme can be implemented efficiently [18].
3. LOCC upperbound

To obtain an upper bound to the LOCC fidelity let us consider a slightly modified communication protocol in which the space explorers are told about what specific preparation of (7) is being used. We will assume that the carrier state is prepared (and that the space explorers are informed accordingly) following this recipe: with probability $p$ the carrier state is $\rho_i = [J, J]_\vec{n}$, i.e. it has total angular momentum $J$ and points to the right (but unknown to the explorers!) direction, whereas with probability $1 - p$ it is $\rho_b \propto \sum_{\alpha} [J - 1, -J + 1, \alpha]_\vec{n} = \sum_{\alpha} [J - 1, J - 1, \alpha]_{-\vec{n}}$, i.e. it has total angular momentum $J - 1$ and points the opposite way. Because of this additional information, the fidelity of the original protocol must be upper bounded by that of the modified one, whose calculation will be carried out below.

From the discussion in the previous paragraph, it is clear that the space explorers have to be able not only to estimate the axis containing the unknown direction and its opposite with good accuracy, but also to discriminate between states with angular momentum $J$ and $J - 1$ (i.e. detect the presence of a singlet $\psi^-$ in the carrier state); note that if $\rho_i$ and $\rho_b$ had both the same angular momentum, say $J$, it would be impossible for the space explorers to gather any information about $\vec{n}$ (on average) since in this case $\rho(\vec{n}) = \rho(-\vec{n})$. We can view $J$ and $J - 1$ as tags that tell the explorers to move forward or backwards relative to the direction they guess from the outcomes of their measurements. Hopefully this guess will be close to the unknown vectors $\vec{n}$ or $-\vec{n}$, respectively. Since the explorers’ ability to estimate the secret direction is conditioned to their ability to read these tags, or more precisely, to their ability to discriminate between spin-$J$ and spin-($J - 1$) states, they have to optimize their measurements to give both a good estimate of the direction in which the state is pointing, and also a low error probability of discrimination between the two possible tags (‘forward’ if $j = J$ versus ‘backwards’ if $j = J - 1$). Actually, our aim is to show that the upper bound of this modified protocol is strictly less than unity. Thus, to simplify the calculation, we will not take into account the difficulties of estimating the direction.

We divide the set $\mathcal{M}$ of POVM elements into two groups, $\mathcal{F}$ and $\mathcal{B}$ (after ‘forward’ and ‘backwards’): those for which the final guess and the measured direction coincide and those for which they are opposite (corresponding to the case where the explorers judge that the input state had total angular momentum $J - 1$). It is clear that the wrong assignments will result in a negative contribution to $\Delta$—at least on average. We can thus obtain a rough upper bound by assuming that (i) $\Delta_{n, \chi} = 1$ when the explorers correctly identify the signal state and (ii) $\Delta_{n, \chi} = 0$ if they fail to do so. In the asymptotic limit, $N \to \infty$, we have that $p = 1/2$, and $\Delta$ is thus bounded by the probability $p_S$ of discriminating between the $J$ and $J - 1$ subspaces:

$$\Delta \leq \frac{1}{2} \left[ \sum_{M_j \in \mathcal{F}} \text{Tr} \left( M_j \frac{1}{d_j} \right) + \sum_{M_j \in \mathcal{B}} \text{Tr} \left( M_j \frac{1}{d_{j-1}} \right) \right]$$

$$= \frac{1}{2} \left[ \frac{1}{d_j} \text{Tr}(Q_j 1_j) + \frac{1}{d_{j-1}} \text{Tr}(Q_{j-1} 1_{j-1}) \right] =: p_S,$$  \hspace{1cm} (9)

where $1_j$ stands for the identity restricted to the spin-$j$ subspace, whose dimension is $d_j = n_j \times (2j + 1)$. In obtaining (9), we have used Schur’s lemma and implicitly defined the local discrimination POVM $Q = \{Q_j, Q_{j-1}\}$. This bound is rough, but of course is saturated for collective POVM since in this case one can perfectly discriminate between the spin-$J$ and
spin-\((J - 1)\) subspaces. Notice also that the bound will not be tight for local measurements since typically one cannot avoid having negative contributions to the fidelity when the explorers fail to discriminate between those subspaces.

Let us now give a bound on \(p_S\), i.e. on the probability that \(Q_J\) and \(Q_{J-1}\) project successfully on the spin-\(J\) and spin-\((J - 1)\) subspaces, respectively. We first notice that any optimal POVM can be locally symmetrized by the action of the rotation group. The weights of every POVM element on each invariant subspace will remain untouched under this action. Hence, for our purposes we can now take

\[
Q_J = a \mathbb{1}_J + b \mathbb{1}_{J-1} + c \mathbb{1}_{J<J-1}; \quad Q_{J-1} = \mathbb{1} - Q_J.
\]

The action of \(Q\), if it ought to be LOCC, cannot produce entanglement. By performing \(Q\) on a conveniently chosen separable probe state and imposing that the resulting state cannot be entangled, we find certain constraints on \(a\) and \(b\), which in turn will give a bound on the discrimination probability. The state we choose is a four-party pure state \(|\psi\rangle_{1234}^\perp\) that is separable with respect to the partition \(((12), (34))\) (see figure 1). More precisely, \(|\psi\rangle_{1234}^\perp = |\psi^+\rangle_{13}^\perp |\psi^+\rangle_{24}^\perp\), where \(|\psi^\perp\rangle_{\mu\nu} = (|0\rangle^\nu |1\rangle^\mu + |1\rangle^\nu |0\rangle^\mu)/\sqrt{2}\), with \(|k\rangle = |J/2, J/2 - k\rangle\). By performing the LOCC measurement \(Q\) on parties 12, which we denote by \(Q_{12}^\perp\), one cannot create entanglement between parties 34. The state of the latter conditioned to having obtained the outcome \(J\) has the form \(\text{Tr}_{12}[Q_{12}^\perp |\psi\rangle_{1234}^\perp \langle \psi|] = a\rho_{34}^\perp + b\rho_{34}^\perp + c\rho_{34}^\perp\), where \(\text{Tr}_{12}\) is the partial trace over parties 12—and an analogous expression is obtained for the outcome \(J - 1\). Using the partial transposition criteria on these states we obtain necessary conditions for them to be separable. Maximizing \(p_S = (1 + a - b)/2\) subject to these conditions we find an upper bound for the fidelity \(\Delta < p_S < 2 - \sqrt{5}/2 = 0.88 < 1\) which holds for all \(N\). Larger values for \(\Delta\) would necessarily imply generation of entanglement by the LOCC protocol we have just discussed.

Figure 1. (A) Schematic representation of the state used in section 3 to obtain the upper bound of the fidelity. The wavy lines represent entanglement between parties. (B) A LOCC measurement on parties (12) cannot create entanglement in parties (34).
4. LOCC lowerbounds

The point of showing the previous bound is that it proves the existence of a finite gap even in the limit $N \to \infty$. We will now present some results that suggest that the gap is in fact very large, corresponding to a LOCC fidelity that is lower than that of a single spin-1/2 pure state. We will do this by studying a sensible family of LOCC estimation protocols. Strictly speaking this will only give a lower bound to the LOCC fidelity. However, as will become apparent below, this is arguably the maximum fidelity attainable by LOCC in the asymptotic limit.

It is now clear that one needs to learn whether the direction is encoded in the $J$ or $J-1$ subspace, i.e. a good protocol has to be able to detect the presence of a singlet in an otherwise fully symmetric state. It is also clear that if the axis $\pm \vec{n}$ is known, one can detect the presence of the singlet by measuring each spin along $\pm \vec{n}$ (if all but one of the outcomes are identical the signal state is in the $J-1$ subspace). The measurement $\{M(\vec{s}, x)\}$ we propose consist of a two step process where we first try to determine the axis $\pm \vec{s}$ of the encoded direction by performing measurements on the first $N_0$ spins. In a second step, one measures the projections of the remaining $N_1 = N - N_0$ spins along the estimated axis ($\pm \vec{s}$) so as to detect the presence of the singlet. Using this scheme, or any other LOCC scheme, one cannot reach $F = 1$ mainly for two reasons: (i) the singlet state may involve one or two of the $N_0$ spins of the first step and thus it may pass unnoticed, (ii) the axis can only be estimated with a precision of $(\Delta \theta)^2 = 4/N_0$, which blurs the effect of a singlet at the second measurement step.

We formalize the above strategy by a POVM on $(\mathbb{C}^2)^{\otimes N_0} \otimes (\mathbb{C}^2)^{\otimes N_1}$ that strictly speaking is semi-local. This will enable us to obtain a closed form for the fidelity without actually giving up locality in the asymptotic limit, since this POVM can be realized by LOCC with arbitrary accuracy as $N_0 \to \infty$ (see below). The POVM elements are given by, $M(\vec{s}, x) = O(\vec{s}) \otimes E(\vec{s}, x)$, where

$$O(\vec{s}) = (N_0 + 1)[J_0, J_0]_{\vec{s}} + (N_0 - 1) \sum_{\alpha=1}^{N_0-1} [J_0 - 1, J_0 - 1, \alpha]_{\vec{s}}; \quad J_0 = \frac{N_0}{2},$$

(10)

define an optimal (and covariant) POVM to estimate the axis, but does not reveal the total angular momentum. The operators $E(\vec{s}, x)$, acting on the last $N_1$ particles, correspond to measuring the projection of the spin along $\vec{s}$ on each of the particles, where $x$ is the total number of ‘up’ outcomes. It can also be written as:

$$E(\vec{s}, x) = \sum_{\{x_i\}: \sum_i x_i = x} \left( \bigotimes_{i=1}^{N_1} \left[ \frac{1}{2} + (-1)^{x_i} \vec{s} \cdot \vec{\sigma} \right] \right) = \sum_{\{x_i\}: \sum_i x_i = x} \left( \bigotimes_{i=1}^{N_1} [1/2, 1/2 - x_i]_{\vec{s}} \right) = [J_1, J_1 - x]_{\vec{s}} \bigoplus_{\beta=1}^{N_1-1} [J_1 - 1, J_1 - x, \beta]_{\vec{s}} + \cdots.$$

The guess associated to $M(\vec{s}, x)$ is $(-1)^{f(x)} \vec{s}$, i.e. $\vec{s}$ determines the axis of the explorers’ guess, while the function $f$, from $\{0, 1, \ldots, N_1\}$ to $\{0, 1\}$, determines its orientation or, in other words, their guess for the tag $j \in \{J, J-1\}$. 

New Journal of Physics 9 (2007) 244 (http://www.njp.org/)
Using the Clebsch–Gordan (coefficients of the) decomposition of the tensor product representation $J_0 \otimes J_1$ one can calculate the matrix elements of $\Omega = O(\vec{z}) \otimes E(\vec{z}, x)$ that are relevant to (4):

$$\Omega(x)^{(J)} = (N_0 + 1) \frac{N_1!(N-x)!}{N!(N_1-x)!} [J, J-x]_z \cdots,$$

$$\Omega(x)^{(J-1)} = (N_0 + 1) \frac{N_0(N-1)x N_1!(N-x)!}{N!(N-x)} \frac{N_1!(N-x)!}{N!(N_1-x)!} [J-1, J-x, 0]_z$$

$$+ (N_0 - 1) \frac{N(N-1)}{(N-x)(N-x-1)} \frac{N_1!(N-x)!}{N!(N_1-x)!} \left\{ \sum_{\alpha=1}^{N_0-1} [J-1, J-x-1, \alpha]_z \right\}$$

$$+ (N_0 + 1) \left\{ \frac{(N_1-x)(N-1)N_1!(N-x)!}{N!(N_1-x)!} \sum_{\beta=1}^{N_1-1} [J-1, J-x, \beta]_z \right\}.$$

With this,

$$\Delta = \frac{N_1!}{2N!} \sum_x (-1)^{f(x)} \frac{(N-x)!}{(N_1-x)!} \left\{ \left( \frac{N_0+1}{N+1} \right)^N \left( \frac{N+x}{N+2} \right)^{N-x} - \frac{1}{N(N-1)(N-x)} \right\}$$

$$+ \left( \frac{N-2x-2}{N-x-1} \right)^N \left[ (N-2x)(1-x) \frac{N(N_0+1)}{N_1} \right].$$ \hspace{1cm} (11)

where for simplicity we have taken $p = 1/2$. The sum runs from $x = 0$ up to $x = N_1$ for all the terms but the very last one, for which $1 \leq x \leq N_1$. In the asymptotic limit this expression is maximized by taking $f(x) = 0$ for $x = 0$, $N_1$ and $f(x) = 1$ otherwise, and by taking $N_1 = N_0 = N/2$. One obtains $\Delta_{\text{max}} = 1/4 + 1/(2N) + O(N^{-3})$. Interestingly, we notice that the fidelity decreases with the number $N$ of spins, which reflects the fact that it becomes increasingly difficult to detect a singlet among a growing number of parallel spins.

We next show that the covariant part of the above protocol can actually be carried out using LOCC. Let us start by considering the problem of estimating $\vec{n}$ given the state

$$\rho' = q[J_0, J_0]_{\vec{n}} + \frac{1-q}{N_0 - 1} \sum_{\alpha} [J_0 - 1, J_0 - 1, \alpha]_{\vec{n}}.$$ \hspace{1cm} (12)

For any protocol (any LOCC or covariant POVM $\mathcal{M}$) such that

$$\Delta = 1 - J_0^{-1} + O(J_0^{-1-a}); \quad 1 \geq a > 0,$$ \hspace{1cm} (13)

independently of $q$, one can show that for $j = J_0, J_0 - 1$

$$\frac{\Omega_{jj}}{2j+1} = 1 - O(j^{-a}); \quad \frac{\Omega_{mm}}{2j+1} = O(j^{-a}) \quad \text{if} \ m \neq j.$$

Hence, in the limit $N_0 \to \infty$, these matrix elements coincide with those of $\Omega = O(\vec{z})$, corresponding to the POVM $\{O(\vec{z})\}$ in (10). It is easy to verify that the LOCC state estimation protocol of [19], which is optimal for pure state estimation, also fulfills the condition (13) when applied to the state $\rho'$ in (12). In this protocol one uses a vanishing fraction of the $N_0$ parties to get a rough estimate of $\vec{n}$ (by standard tomography, for instance). In a second stage one uses
Figure 2. The fidelity for different protocols (see main text for detailed explanation): joint measurements (solid), which is the optimal protocol; local adaptive projective measurements (triangles); semi-local covariant protocol of equation (11) (dashed); standard tomography for direction estimation applied on a fraction of the parties followed by a measurement of the spins of the remaining parties along the estimated axis (dotted).

for the remaining parties to refine the estimation by measuring projections of the spin on the plane orthogonal to the rough estimate. We thus conclude that there exists a LOCC measurement strategy that achieves

\[ \Delta_{\text{LOCC}} = \frac{1}{4} + \mathcal{O}(N^{-a}). \]  

(14)

This very same protocol can be used to discriminate between the $J$ and $J-1$ subspaces, i.e. between two arbitrary unknown states belonging to each subspace, with probability of success $p_s = 5/8$. This follows from the fact that any two states belonging to the $J$ and $J-1$ subspaces can be respectively brought to $\mathbb{1}_J/d_J$ and $\mathbb{1}_{J-1}/d_{J-1}$ by applying a random global rotation on all spins, which is a local operation. Such states allow for an ensemble interpretation in terms of isotropically distributed states $\ket{J, J}_n$ and $\ket{J-1, J-1}_n$. Therefore we can blindly apply the above protocol using the function $f(x)$ to assign each measurement outcome to one of the two input states.

Notice that the leading order in (14) can be easily accounted for by the relation

\[ \Delta_{\text{LOCC}} \approx p_s \Delta_J - (1 - p_s) \Delta_{J-1} \approx 2p_s - 1 = 1/4, \]

where $\Delta_J$ and $\Delta_{J-1}$ correspond to the fidelity obtained when the input state is $\ket{J, J}_n$ and $1/(N-1) \sum_\alpha [J-1, J-1, \alpha]_n$, respectively, and in both cases $\Delta_J \approx \Delta_{J-1} \approx 1$. This means that an error in discriminating between the invariant subspaces (the tags), has a very important negative impact on the fidelity. For this reason, the upper bound (9) is far from being tight.

In figure 2, we show the fidelity $F = (1 + \Delta)/2$ for different measurement schemes. The fidelity obtained by joint measurements (solid line in the figure) clearly shows that this scheme outperforms all the others, and is the only one that reaches unity asymptotically. Finding the optimal LOCC scheme is an extremely difficult task even for finite $N$, since it can in principle include an infinite sequence of weak measurements with back and forward rounds.
of communication between them. Instead, we show the fidelity for the following schemes, which we expect to approximate the optimal LOCC value: with triangles, we represent the values obtained with the most general sequence of local adaptive projective measurements [20], which due to the increasing numerical complexity is limited to \( N \leq 7 \). Such protocols do not exhaust the whole class of LOCC schemes, but their fidelity has been shown to be very close or coincide with that of the optimal LOCC schemes in standard state estimation problems [20]. The dashed lines represents the fidelity of the semi-local protocol given in (11). Here, the use of non-local measurements is limited to the estimation of the axis without unveiling the value of \( j \). We thus expect this protocol to mimic very well the best LOCC strategy. Moreover, as shown above, its fidelity can be reached asymptotically with a strictly local strategy. The dotted curve represents the fidelity when standard tomography (i.e. measurements along three fixed orthogonal directions) is used to estimate the axis in the first stage of the protocol (instead of the non-local measurement of the previous protocol). As before, we have optimized over the number of copies used in each stage. We note that all (semi-)local protocols give similar fidelities which, moreover, fall way below that of a single spin, \( F_1 = \frac{2}{3} \). Note also that tomography performs slightly worse than the semi-local (but asymptotically fully local) protocol. This can be traced back to the value of the sub-leading term in the asymptotic expression of \( \Delta_1 \): from [20] we have \( 1 - \Delta = 6/(5j) \), which is larger than the value \( 1/j \) required for (14) to hold.

5. Robustness

We finish by studying the robustness of the optimal state when a number \( M \) of parties is left out. A long but straightforward calculation shows that after tracing out a fraction \( \xi \) of parties, \( \xi = \lim_{N \to \infty} M/N \), the optimal fidelity can be written as

\[
F = 1 - \frac{\xi}{2} - \left( 1 + \frac{\xi}{2} \right) \frac{1}{N} + \frac{1 + \xi + \xi^2/2}{1 - \xi} \frac{1}{N^2} + \cdots.
\]

(15)

So, in the case that the fraction of lost parties is vanishingly small (\( \xi \to 0 \)), the fidelity remains the same up to \( O(N^{-1}) \), while it falls below unity already at the leading order for a non-vanishing fraction.

6. Conclusions

We have presented a quantum communication protocol that provides a way to share a secret spatial direction among several parties with the promise that they cannot learn the direction if they perform LOCC, but can retrieve it with the accuracy of a ‘classical’ gyroscope (of spin \( J = N/2 \)) if they perform collective measurements. The absence of a shared reference frame between sender and receivers implies that the information cannot be encoded on arbitrary qubit states but on a system carrying angular momentum. Most quantum communication protocols require common reference frames, therefore a direction hiding protocol could be primitive to establish such frames without compromising the security requirements. Finally, from a more technical perspective, our results add new insights into the problem of state estimation on correlated copies, and provide bounds on the probability of locally discriminating states with different angular momentum in many-body systems. The latter might have implications in other fields of research. We have supplied evidence that the proven bounds might be made much tighter.
Acknowledgments

We are grateful to A Acin, S Barnett, S Popescu and W Wooters, and especially to A Monràs for discussions. We acknowledge financial support from the Spanish MCyT, under Ramón y Cajal program (JC), CONSOLIDER2006-00019 and FIS2005-01369 and CIRIT SGR-00185. RDD acknowledges support from Foundation for Polish Science, the MNiI under PBZ-Min-008/P03/03 and the EC Program QUPRODIS.

References

[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Rev. Mod. Phys. 74 145
[2] Cleve R, Gottesman D and Lo H K 1999 Phys. Rev. Lett. 83 648
   Hillery M, Bužek V and Berthiaume A 1999 Phys. Rev. A 59 1829
   Gottesman D 2000 Phys. Rev. A 61 042311
[3] Terhal B M, DiVincenzo D P and Leung D W 2001 Phys. Rev. Lett. 86 5807
   Eggeling T and Werner R F 2002 Phys. Rev. Lett. 89 097905
   Hayden P, Leung D and Smith G 2005 Phys. Rev. A 71 062339
[4] Peres A and Scudo P F 2001 Phys. Rev. Lett. 87 167901
   Bagan E, Baig M and Munoz-Tapia R 2001 Phys. Rev. Lett. 87 257903
   Rudolph T and Grover L 2003 Phys. Rev. Lett. 91 217905
[5] Verstraete F and Cirac J I 2003 Phys. Rev. Lett. 91 010404
   Kitaev A, Mayers D and Preskill J 2004 Phys. Rev. A 69 052326
   Bartlet S D, Rudolph T and Spekkens R W 2004 Phys. Rev. A 70 032307
   [6] Bartlett S D, Rudolph T and Spekkens R W 2007 Rev. Mod. Phys. 79 555
[7] Bartlett S D, Rudolph T and Spekkens R W 2003 Phys. Rev. Lett. 91 027901
   van Enk S J 2005 Phys. Rev. A 71 032339
[8] Paris M and Rehzek J 2004 Quantum State Estimation (Lecture Notes in Physics vol 649) (Springer: Berlin)
   Helstrom C W 1976 Quantum Detection and Estimation Theory (Academic: New York)
[9] Horodecki P 2003 Phys. Rev. Lett. 90 167901
[10] Banaszek K 2001 Phys. Rev. Lett. 86 1366
[11] Bruß D, Ekert A and Macchiavello C 1998 Phys. Rev. Lett. 81 2598
   Bae J and Acin A 2006 Preprint quant-ph/0603078
[12] Bacon D, Childs A M and van Dam W 2005 Proc. 46th IEEE Symposium on Foundations of Computer Science (FOCS 2005) pp 469–78 Preprint quant-ph/0504083
[13] Demkowicz-Dobrzański R 2005 Phys. Rev. A 71 062321
[14] Bagan E, Baig M, Brey A, Munoz-Tapia R and Tarrach R 2000 Phys. Rev. Lett. 85 5230
[15] Bagan E, Ballester M A, Gill R D, Monras A and Munoz-Tapia R 2006 Phys. Rev. A 73 032301
[16] Edmonds A R 1960 Angular Momentum in Quantum Mechanics (Princeton University Press: Princeton)
[17] Massar S and Popescu S 1995 Phys. Rev. Lett. 74 1259
[18] Bacon D, Chuang I and Harrow A 2004 Preprint quant-ph/0407082
[19] Gill R D and Massar S 2000 Phys. Rev. A 61 042312
[20] Bagan E, Baig M and Munoz-Tapia R 2002 Phys. Rev. Lett. 89 277904
   Bagan E, Monras A and Munoz-Tapia R 2005 Phys. Rev. A 71 062318