Information–disturbance tradeoff in sending direction information via antiparallel quantum spin

2010 J. Phys. A: Math. Theor. 43 235301

(http://iopscience.iop.org/1751-8121/43/23/235301)

J. Phys. A: Math. Theor. **43** (2010) 235301 (9pp) doi:10.1088/1751-8113/43/23/235301

Information–disturbance tradeoff in sending direction information via antiparallel quantum spin

ShengLi Zhang[1], **XuBo Zou**[1], **ChuanFeng Li**[1], **ChenHui Jin**[2] **and GuangCan Guo**[1]

[1] Key Laboratory of Quantum Information, University of Science and Technology of China (CAS), Hefei 230026, People's Republic of China
[2] Electronic Technology Institute, Information Engineering University, Zhengzhou, Henan 450004, People's Republic of China

E-mail: xbz@ustc.edu.cn

Received 24 July 2009, in final form 5 April 2010
Published 13 May 2010
Online at stacks.iop.org/JPhysA/43/235301

Abstract
When sending unknown direction information, antiparallel spins contain more direction information than parallel spins (Gisin and Popescu 1999 *Phys. Rev. Lett.* **83** 432). In this paper, the optimal information–disturbance tradeoff bound for antiparallel spins is derived. The quantum measurements which attain the optimal tradeoff bound are obtained. This result can be of practical relevance for posing some general limits on Eve's eavesdropping process. Finally, we also present a comparison between the bound for antiparallel spins and the bound for parallel spins.

PACS numbers: 03.67.−a, 03.65.Ta

(Some figures in this article are in colour only in the electronic version)

1. Introduction

With a pre-established reference frame between two remote users, Alice and Bob, an unknown direction information $\vec{n}$ can be encoded with a series of classical bits and can then be exchanged conveniently via quantum or classical channels. However, there are many cases when such a reference frame is not available and all that we can do is to send a natural object, such as a gyroscope pointing in a direction, to share the direction information. In the realm of quantum information, quantum mechanical spin polarized along the direction, $\vec{n}$, has been considered as a promising candidate for such a natural object and for establishing such a shared direction [1, 2].

Since the seminal work by Peres and Wootters [3], a considerable effort has been made in the literature to derive the optimal strategy in sending and receiving direction information

[4–13]. With a single quantum spin, the optimal procedure for encoding and decoding direction information is obvious and straightforward—Alice simply uses a spin pointing to $\vec{n}$ to encode the direction, and the optimal measurement strategy for Bob is a standard Stern–Gerlach measurement, along an arbitrary direction $\vec{m}$ [9]. While, for two quantum spins, Gisin and Popescu showed that antiparallel spins contain more direction information than parallel spins [10]. Recently, it was shown that antiparallel spins provide the maximal transmission fidelity [12].

However, all these studies in the transmission of direction information are aimed at the maximization of the transmission fidelity, namely at determining as accurately as possible the direction in which the spins are pointing. In the real world, particularly in the presence of potential eavesdropper (Eve), it is often of great importance to make a security analysis of the extent to which Eve could have tapped the shared direction information. In this paper, we will use the information–disturbance tradeoff bound [14] as the basic tool and give a quantitative bound on Eve's eavesdropping process.

In fact, the tradeoff between information gain and state disturbance is one of the fundamental rules in quantum mechanics. There is not a quantum measurement on an unknown quantum system without introducing any disturbance. There exists a quantitative tradeoff between information gain and state disturbance [14–21]. More importantly, the tradeoff which is inherited by quantum mechanics is applicable to any measurement observer, including Bob and any eavesdropper, and thus imposes a general limit on the information eavesdropping in quantum communications.

This paper is organized as follows. In section 2, we will give a mathematical description of the tradeoff bound between information and disturbance for antiparallel spins. In section 3, we will give a derivation of the optimal tradeoff bound with the group covariant technique and vector analysis technique. Then, both the optimal group covariant measurement and discrete positive operator value measure (POVM) measurement are presented in section 4. Finally, we give a comparison between the tradeoff bound for antiparallel and parallel spins in section 5. Section 6 follows the conclusion.

2. Information–disturbance bound in quantum measurement of antiparallel spins

Let us now give a general formalism of the information disturbance problem. Assuming that the state $|\psi\rangle$ is homogeneously picked from a given state set Ω, we just perform a measurement on this unknown state and then determine what the state will be based on our measurement outcome. On the one hand, with the measurement outcome, we can obtain some information gain about the unknown state. On the other hand, after the measurement, the unknown state will be distorted. Quantum mechanics imposes some constraints on the relation between the information gain $\mathcal{I}$ and the state disturbance $\mathcal{D}$ (introduced by quantum measurement). For a given value of $\mathcal{D}$, there exists an upper bound value for $\mathcal{I}$ and no physically available measurement can be found to beat such a bound. The exact tradeoff bound between $\mathcal{I}$ and $\mathcal{D}$ is naturally imposed by quantum mechanics and is what we are mainly concerned with here.

First of all, let us establish a one–one correspondence between the direction $\vec{n}$ and antiparallel quantum spins. As shown by Gisin and Popescu [10], one can use the antiparallel spins state $|\vec{n}\rangle|-\vec{n}\rangle$ to encode the unknown direction $\vec{n}$. In order to apply the group covariant technique in our derivation, for convenience, we will identify Alice's direction $\vec{n}$ with a group parameter $g \in \mathbb{G} = \mathrm{SU}(2)$. In fact, with a fixed direction $\vec{n}_0$, every direction, $\vec{n}$, can be represented as a result of a certain unitary rotation g acting on a fixed direction $\vec{n}_0$:

$$\vec{n} = g\vec{n}_0. \tag{1}$$

In our following calculation, we will rewrite the state $|\vec{n}\rangle$ as

$$|\vec{n}\rangle \equiv |\psi(g)\rangle \equiv U_g|\psi(0)\rangle, \tag{2}$$

where U_g denotes the unitary group representation for $SU(2)$ and $|\psi(0)\rangle$ is the state corresponding to $\vec{n}_0$. For example, one can choose $\vec{n}_0 = (n_x, n_y, n_z) = (0, 0, 1)$ as the reference direction and the eigenstate of $\vec{n}_0 \cdot \vec{\sigma} = \sigma_z$ as $|\psi(0)\rangle$, i.e. [6]

$$\vec{n}_0 \cdot \vec{\sigma}|0\rangle = |0\rangle, \qquad |\psi(0)\rangle \equiv |0\rangle. \tag{3}$$

Following the definitions of equations (2) and (3), the antiparallel spins $|\vec{n}\rangle|-\vec{n}\rangle$ can be conveniently expressed with the state $|\psi(g)\rangle|\psi(g)^{\perp}\rangle$, where $|\psi(g)^{\perp}\rangle$ denotes the orthogonal state of $|\psi(g)\rangle$. Correspondingly, the set Ω boils down to a collection of antiparallel states

$$\Omega = \{|\Psi_g\rangle \equiv |\psi(g)\rangle|\psi(g)^{\perp}\rangle,\ g \in SU(2)\}. \tag{4}$$

For the unknown state $|\Psi_g\rangle$ in equation (4), without loss of generality, we can assume that the most generalized quantum measurement, i.e. a set of *completely positive trace preserving* (CPTP) maps $\{\mathcal{E}_r\}$ [22, 23] is performed to retrieve the information of the group parameter g, namely the unknown direction information $\vec{n}$. The measurement is generally probabilistic: each measurement outcome r denotes a map from the input state $|\Psi_g\rangle$ to the output state $\varrho'_{rg} = \mathcal{E}_r(|\Psi_g\rangle\langle\Psi_g|)/p_{rg}$. Here, $p_{rg} = \mathrm{Tr}[\mathcal{E}_r(|\Psi_g\rangle\langle\Psi_g|)]$ is a normalization factor and represents the probability with which the measurement outcome r is observed. More precisely, we introduce here Kraus's operator-sum theory [23] and give the operator decomposition to each CP map $\mathcal{E}_r$:

$$\mathcal{E}_r(|\Psi_g\rangle\langle\Psi_g|) = \sum_{\mu} A_{r\mu}|\Psi_g\rangle\langle\Psi_g|A_{r\mu}^{\dagger}, \tag{5}$$

where $A_{r\mu}$ are named as Kraus opeartors. The probability p_{rg} then satisfies

$$p_{rg} = \mathrm{Tr}[\Pi_r|\Psi_g\rangle\langle\Psi_g|], \qquad \Pi_r = \sum_{\mu} A_{r\mu}^{\dagger}A_{r\mu}. \tag{6}$$

In the literature, the set of operator $\{\Pi_r\}$ is known as the positive operator valued measurement (POVM). Furthermore, in the following we will make repetitive use of the trace-preserving condition. This is a prerequisite condition for guaranteeing that the CP maps can be physically available. The condition that $\{\mathcal{E}_r\}$ is trace preserving is equivalent to requiring that $\sum_{r\mu} A_{r\mu}^{\dagger}A_{r\mu} = \mathbb{1} \otimes \mathbb{1}$, where we use $\mathbb{1}$ to denote the identity matrix in the Hilbert Space of single quantum spin.

Now it is our turn to present the detailed definitions for the information gain $\mathcal{I}$ and state disturbance $\mathcal{D}$. In fact, both the information gain and state disturbance will be evaluated with fidelities. With the measurement outcome r, one can make some inference rule $r \to |\psi(r)\rangle$ and infer that $|\psi(r)\rangle|\psi(r)^{\perp}\rangle$ is the quantum state of the input antiparallel spins. Then, the fidelity—the overlap between $|\psi(r)\rangle$ and $|\psi(g)\rangle$—is a good figure of merit for the information gain [19]. Thus, by averaging over all the possible outcome r, the average information $\mathcal{I}_g$ can be given by

$$\begin{aligned}\mathcal{I}_g &= \sum_{r} p_{rg}|\langle\psi(r)|\psi(g)\rangle|^2 \\ &= \sum_{r\mu} \mathrm{Tr}[A_{r\mu}^{\dagger}A_{r\mu}|\Psi_g\rangle\langle\Psi_g|]\mathrm{Tr}[|\psi(g)\rangle\langle\psi(g)|\psi(r)\rangle\langle\psi(r)|].\end{aligned} \tag{7}$$

Similarly, the amount of the disturbance caused by quantum measurement can be quantified with the fidelity between the output state ϱ'_{rg} and the input state $|\psi(g)\rangle|\psi(g)^{\perp}\rangle$. We have

$$\mathcal{D}_g = 1 - \mathcal{F}_g, \qquad \mathcal{F}_g = \langle\psi(g)|\mathrm{Tr}_2[\varrho'_{rg}]|\psi(g)\rangle = \mathrm{Tr}[\varrho'_{rg}|\psi(g)\rangle\langle\psi(g)| \otimes \mathbb{1}], \tag{8}$$

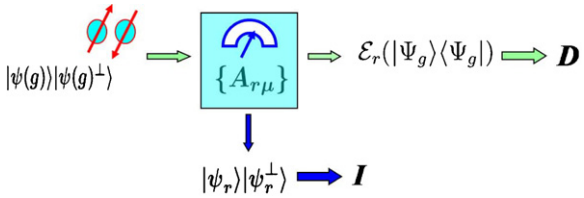

Figure 1. The tradeoff between information gain and state disturbance in the quantum measurement of antiparallel spins.

where Tr_2 denotes a partial trace over the second spins. It should be noted here that we omit the contribution of the second spin since this complies with the definition in the literature [10, 11] and can be conveniently incorporated into the comparison with the parallel spins [24] (see section 5 for more information).

The definitions of $\mathcal{I}_g$ and $\mathcal{D}_g$ are all dependent on the special choice of parameter g. In practice, when the group parameter g is randomly chosen from $SU(2)$, we can evaluate the average information gain and state disturbance by further averaging over all the possible parameter g, or equivalent, over the set Ω:

$$\mathcal{I} = \int_{SU(2)} \mathrm{d}g\mathcal{I}_g, \qquad \mathcal{D} = \int_{SU(2)} \mathrm{d}g\mathcal{D}_g. \tag{9}$$

In figure 1, we present a mathematical model for the information–disturbance tradeoff problem. In the following section, we will use the group covariant technique and vector analysis technique for the optimal Kraus operators $\{A_{r\mu}\}$ and the optimal tradeoff bound between $\mathcal{I}$ and $\mathcal{D}$.

3. Covariant measurement and optimal information–disturbance bound

The group covariant quantum measurement is a special kind of measurement which originates from the symmetry of input state and has already been proven to be optimal in the quantum cloning [25–27] process and quantum state estimation [28]. It can be easily shown that the optimality also preserves in our problem. In fact, for an arbitrary (covariant or non-covariant) CPTP map $\mathcal{E}(\rho) = \sum_{r\mu} A_{r\mu}\rho A_{r\mu}^{\dagger}$, one can construct a covariant CPTP map $\mathcal{E}'(\rho) = \int_h \mathcal{E}'_h(\rho)\,\mathrm{d}h$ which yields the same amount of information gain and disturbance, where $\mathcal{E}'_h(\cdot)$ and the guessed state for the result h are chosen to be

$$\mathcal{E}'_h(\rho) = \sum_{r\mu} \left(U_h U_r^{\dagger} \otimes U_h U_r^{\dagger}\right) A_{r\mu} \left(U_r U_h^{\dagger} \otimes U_r U_h^{\dagger}\right) \rho \left(U_h U_r^{\dagger} \otimes U_h U_r^{\dagger}\right) A_{r\mu}^{\dagger} \left(U_r U_h^{\dagger} \otimes U_r U_h^{\dagger}\right), \tag{10}$$

$$|\psi(h)\rangle = U_h|0\rangle, \tag{11}$$

respectively, with the subscript $h \in SU(2)$ denoting the measurement result of the continuous POVM. Therefore, the optimal tradeoff bound for the covariant map is also the optimal bound for arbitrary maps. Therefore, in searching for the optimal bound between $\mathcal{I}$ and $\mathcal{D}$, there will be no loss of generality if we confine our study within the covariant quantum measurements.

The covariant map in equations (10) and (11), along with its good property $\mathcal{E}'_{gh}(\rho) = U_g \mathcal{E}_h\left(U_g^{\dagger}\rho U_g\right)U_g^{\dagger}$, not only guarantees that the measurement achieves its optimal performance for all the possible state $|\Psi_g\rangle$, but also simplifies our following computation, considerably.

Hereafter, we will consider the covariant instrument

$$A_h = U_h \otimes U_h A_0 U_h^\dagger \otimes U_h^\dagger \tag{12}$$

with the operator A_0 denoting a seed of the whole set of Kraus operators. The optimal tradeoff between information and disturbance can now be obtained by optimizing the operator A_0.

Note that the trace-preserving condition now boils down to $\int_h A_h^\dagger A_h = \mathbb{1} \otimes \mathbb{1}$ which can be further simplified with Schur's lemma for reducible group representation [29]:

$$\int_{SU(2)} \mathrm{d}g U_g \otimes U_g A_0^\dagger A_0 U_g^\dagger \otimes U_g^\dagger = \mathrm{Tr}\big[A_0^\dagger A_0 \mathcal{M}_1\big]\mathcal{M}_1 + \mathrm{Tr}\big[A_0^\dagger A_0 \mathcal{M}_2\big]\mathcal{M}_2/3, \tag{13}$$

where $\mathcal{M}_1 = |\Psi^-\rangle\langle\Psi^-|(|\Psi^\pm\rangle = (|01\rangle \pm |10\rangle)/\sqrt{2})$ denotes the uni-dimensional completely asymmetric subspace and $\mathcal{M}_2 = \mathbb{1} \otimes \mathbb{1} - \mathcal{M}_1$ denotes the three-dimensional symmetric subspace. Now the trace-preserving condition boils down to

$$\mathrm{Tr}\big[A_0^\dagger A_0 \mathcal{M}_1\big] = 1, \qquad \mathrm{Tr}\big[A_0^\dagger A_0 \mathcal{M}_2\big] = 3. \tag{14}$$

With the covariant measurement $\{A_h\}$, the integral $\mathrm{d}g$ in equation (9) can easily be obtained. For $\mathcal{D}$, we have

$$\begin{aligned}
\mathcal{D} &= 1 - \int_{\mathbb{G}} \mathrm{d}g \int_{\mathbb{G}} \mathrm{d}h \mathrm{Tr}\big[A_h |\Psi_g\rangle\langle\Psi_g| A_h^\dagger |\psi(g)\rangle\langle\psi(g)| \otimes \mathbb{1}\big] \\
&= 1 - \sum_{i=0,1} \int_{\mathbb{G}} \mathrm{d}g \langle\psi(g)|\langle i|A_0|\Psi_g\rangle\langle\Psi_g|A_0^\dagger|\psi(g)\rangle|i\rangle \\
&= 1 - \sum_{i,j,k=0,1} \int_{\mathbb{G}} \mathrm{d}g \langle\psi(g)|(|j\rangle\langle j|)\langle i|A_0|\Psi_g\rangle\langle\Psi_g|A_0^\dagger|k\rangle\langle k|\psi(g)\rangle|i\rangle \\
&= 1 - \sum_{i,j,k=0,1} \langle ji|A_0 M_{jk} A_0^\dagger|ki\rangle,
\end{aligned} \tag{15}$$

where the operator

$$M_{jk} = \int_{\mathbb{G}} \mathrm{d}g \langle\psi(g)|j\rangle \cdot |\Psi_g\rangle\langle\Psi_g| \cdot \langle k|\psi(g)\rangle, \qquad j,k \in \{0,1\} \tag{16}$$

can be calculated explicitly with the Schur lemma. With some algebra, we obtain that

$$M_{00} = (|0\rangle\langle 0| \otimes \mathbb{1} + \mathbb{1} \otimes |1\rangle\langle 1|)/12 + |\Psi^-\rangle\langle\Psi^-|/6, \tag{17}$$

$$M_{11} = (\mathbb{1} \otimes |0\rangle\langle 0| + |1\rangle\langle 1| \otimes \mathbb{1})/12 + |\Psi^-\rangle\langle\Psi^-|/6, \tag{18}$$

$$M_{01} = M_{10}^\dagger = (|\Psi^-\rangle\langle 11| - |00\rangle\langle\Psi^-|)/6\sqrt{2}. \tag{19}$$

The derivation for $\mathcal{I}$ can be done in a similar way, which yields

$$\begin{aligned}
\mathcal{I} &= \int_{\mathbb{G}} \mathrm{d}g \int_{\mathbb{G}} \mathrm{d}h \mathrm{Tr}\big[A_h^\dagger A_h |\Psi_g\rangle\langle\Psi_g|\big] \big|\langle 0|U_h^\dagger U_g|0\rangle\big|^2 \\
&= \int_{\mathbb{G}} \mathrm{d}g \mathrm{Tr}\big[A_0^\dagger A_0 |\Psi_g\rangle\langle\Psi_g|\big] \cdot \langle\psi(g)|0\rangle\langle 0|\psi(g)\rangle \\
&= \mathrm{Tr}\big[A_0^\dagger A_0 M_{00}\big] = \frac{1}{3} + \frac{1}{6\sqrt{2}}\big(\langle\Psi^-|A_0^\dagger A_0|01\rangle + \langle 01|A_0^\dagger A_0|\Psi^-\rangle\big).
\end{aligned} \tag{20}$$

Now putting all these results together, the tradeoff problem can be re-formulated with the following semi-definite programming problem:

$$\mathrm{Min}_{A_0} : 1 - \sum_{i,j,k=0,1} \langle ji|A_0 M_{jk} A_0^\dagger|ki\rangle \tag{21}$$

such that

$$\mathcal{I} = \mathrm{Tr}\big[A_0^\dagger A_0 M_{00}\big], \qquad A_0^\dagger A_0 \geqslant 0, \qquad \mathrm{Tr}\big[A_0^\dagger A_0 \mathcal{M}_1\big] = 1, \qquad \mathrm{Tr}\big[A_0^\dagger A_0 \mathcal{M}_2\big] = 3. \tag{22}$$

To continue our derivation, we will rely on the vector analysis technique and derive the optimal tradeoff bound. First, we need to introduce a few vectors $\{\vec{\mathbf{v}}_i = \{v_{i1}, v_{i2}\}^{\mathrm{T}}, v_{ij} \in \mathbb{C}\}$ $(i = 1, 2, \ldots, 8,\ j = 1, 2)$ such that

$$A_0 = \left(\begin{array}{c|c|c|c} a_{11} & a_{12} & a_{13} & a_{14} \\ \hline a_{21} & a_{22} & a_{23} & a_{24} \\ \hline a_{31} & a_{32} & a_{33} & a_{34} \\ \hline a_{41} & a_{42} & a_{43} & a_{44} \end{array}\right) = \left(\begin{array}{c|c|c|c} \vec{\mathbf{v}}_1 & \vec{\mathbf{v}}_2 & \vec{\mathbf{v}}_3 & \vec{\mathbf{v}}_4 \\ \hline \vec{\mathbf{v}}_5 & \vec{\mathbf{v}}_6 & \vec{\mathbf{v}}_7 & \vec{\mathbf{v}}_8 \end{array}\right). \tag{23}$$

This helps to give much simpler expressions to our problem. First of all, the trace-preserving equation (14) can be reduced to

$$\sum_i |\vec{\mathbf{v}}_i|^2 = 4, \tag{24}$$

$$|\vec{\mathbf{v}}_2 - \vec{\mathbf{v}}_3|^2 + |\vec{\mathbf{v}}_6 - \vec{\mathbf{v}}_7|^2 = 2. \tag{25}$$

Then, it can easily be obtained that

$$\mathcal{D} = \tfrac{1}{2} - \tfrac{1}{12} f, \qquad \mathcal{I} = \tfrac{1}{2} + \tfrac{1}{12} g, \tag{26}$$

with f and g defined by

$$f = |\vec{\mathbf{v}}_2|^2 - |\vec{\mathbf{v}}_3|^2 + |\vec{\mathbf{v}}_7|^2 - |\vec{\mathbf{v}}_6|^2 - |\vec{\mathbf{v}}_1|^2 - |\vec{\mathbf{v}}_8|^2 + |\vec{\mathbf{v}}_7 - \vec{\mathbf{v}}_6 + \vec{\mathbf{v}}_1|^2 + |\vec{\mathbf{v}}_8 + \vec{\mathbf{v}}_2 - \vec{\mathbf{v}}_3|^2 - 2, \tag{27}$$

$$g = |\vec{\mathbf{v}}_2|^2 - |\vec{\mathbf{v}}_3|^2 + |\vec{\mathbf{v}}_6|^2 - |\vec{\mathbf{v}}_7|^2. \tag{28}$$

The optimization in equation (21) can now be equivalently reduced to looking for a set of vectors $\vec{\mathbf{v}}_i$ that satisfy the constraints equations (24) and (25) and maximize f for a given value g.

After some lengthy but not very interesting algebra, one can check that the relation between f and g actually follows

$$f \leqslant g + \sqrt{24 - 2g^2}. \tag{29}$$

This means that for any quantum measurement, the amount of the disturbance $\mathcal{D}$ caused on the quantum states must satisfy

$$\mathcal{D} \geqslant 1 - \mathcal{I} - \sqrt{-\tfrac{1}{3} + 2\mathcal{I} - 2\mathcal{I}^2}, \tag{30}$$

or equivalently,

$$\mathcal{I}_{\mathrm{anti}} \leqslant \tfrac{1}{3}(2 - \mathcal{D} + \sqrt{2\mathcal{D}(1 - \mathcal{D})}). \tag{31}$$

The bound in equation (30) coincides with our intuition: the more information we obtain, the more the state has to be disturbed. For the minimal disturbance measurement, $\mathcal{D} = 0$; we can achieve this by performing the optimal measurements on the second spin only while leaving the first spin undisturbed. However, the information gain from the optimal measurement on the second spin can only achieve up to $\mathcal{I} = 2/3$. If one uses more informative measurement, more disturbance has to be introduced to the input state. In the case of the most informative measurement, $\mathcal{I} = \frac{3+\sqrt{3}}{6}$, as shown in [10], we find from equation (30) that the disturbance as low as $\mathcal{D}(\mathcal{I}) = \frac{3-\sqrt{3}}{6}$ has to be introduced. For the less informative measurement, $2/3 < \mathcal{I} < \frac{3+\sqrt{3}}{6}$, the disturbance $\mathcal{D}$ is given explicitly in equation (30). A plot of the quantitatively tradeoff is shown with dashed line in figure 2(a).

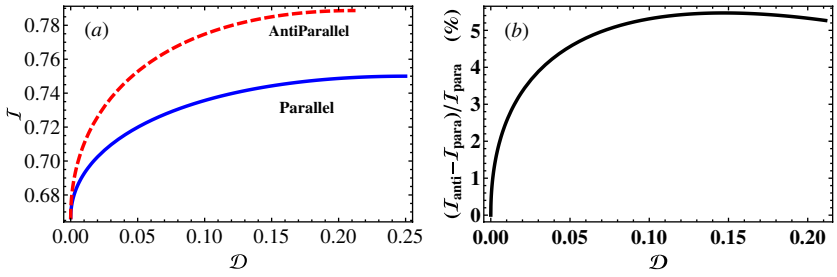

Figure 2. (*a*) Comparative plot of information–disturbance tradeoff between antiparallel (dashed line, equation (31)) and parallel spins (solid line, equation (38)). (*b*) A higher amount of information gain $\Delta\mathcal{I} = (\mathcal{I}_{\text{anti}} - \mathcal{I}_{\text{para}})/\mathcal{I}_{\text{para}}$ as a function of disturbance $\mathcal{D}$. The maximal value of $\Delta\mathcal{I}$ is 5.470% at $\mathcal{D} = 0.147$.

4. Optimal quantum measurement and discrete POVMS

The optimal quantum operation which achieves the tradeoff bound in equation (31) can be deduced from the derivation of equation (29). Here we omit the complicated process and list the main result. In fact, the operators A_0 with

$$\frac{\vec{\mathbf{v}}_2}{|\vec{\mathbf{v}}_2|} = \frac{\vec{\mathbf{v}}_3}{|\vec{\mathbf{v}}_3|} = \frac{\vec{\mathbf{v}}_8}{|\vec{\mathbf{v}}_8|}, \qquad \vec{\mathbf{v}}_1 = \vec{\mathbf{v}}_4 = \vec{\mathbf{v}}_5 = \vec{\mathbf{v}}_6 = \vec{\mathbf{v}}_7 = \vec{\mathbf{0}} \tag{32}$$

is one example at hand. Particularly, we can introduce a control parameter θ ($0 \leqslant \theta \leqslant \arccos(\sqrt{3}/3)$):

$$A_\theta = |00\rangle\langle\Psi^-| + \frac{\sqrt{6}\cos\theta}{2}|00\rangle\langle\Psi^+| + \sqrt{3}\sin\theta|10\rangle\langle 11|. \tag{33}$$

It is straightforward to verify, from equations (15)–(20), that the performance of the covariant measurement, equation (33), follows

$$\mathcal{I} = \frac{1}{2} + \frac{\sqrt{3}}{6}\cos\theta, \tag{34}$$

$$\mathcal{D} = \frac{1}{2} - \frac{\sqrt{3}\cos\theta}{6} - \frac{\sqrt{6}\sin\theta}{6}, \tag{35}$$

and the equality sign in equation (31) can be attained.

Furthermore, by increasing the parameter from 0 to $\arccos(\sqrt{3}/3)$, the covariant measurement $A_h = U_h \otimes U_h A_\theta U_h^\dagger \otimes U_h^\dagger$ interpolates smoothly between the two limiting case of minimal disturbance measurement and the most informative measurement.

From the covariant operators $\{A_h\}$ above, one can also construct a set of discrete POVMs which achieve the same value of $\mathcal{I}$ and $\mathcal{D}$. For example, the measurement with only four Kraus operators can be given by $A_i = \frac{1}{2}U_i \otimes U_i A_\theta U_i^\dagger \otimes U_i^\dagger (i = 0, 1, 2, 3)$ with U_i:

$$U_0 = \mathbb{1}, \qquad U_1 = \tfrac{\sqrt{3}}{3}\mathbb{1} - \mathrm{i}\sigma_y, \tag{36}$$

$$U_2 = \tfrac{\sqrt{3}}{3}\mathbb{1} + \mathrm{i}\tfrac{\sqrt{6}}{6}\sigma_y + \mathrm{i}\tfrac{\sqrt{2}}{2}\sigma_x, \qquad U_3 = \tfrac{\sqrt{3}}{3}\mathbb{1} + \mathrm{i}\tfrac{\sqrt{6}}{6}\sigma_y - \mathrm{i}\tfrac{\sqrt{2}}{2}\sigma_x. \tag{37}$$

It can easily be checked that all these operators satisfy the normalization condition $\sum_i A_i^\dagger A_i = \mathbb{1} \otimes \mathbb{1}$ and the optimal tradeoff for measuring antiparallel states follows equation (31). This

indicates that the relation in equation (29) is exactly a tight one and cannot be improved any more.

5. Comparisons of information–disturbance bounds between antiparallel and parallel spins

Before concluding, we will give a comparison of the information–disturbance tradeoff between antiparallel and parallel spins and then present some discussion about the security capacity of sending direction information via antiparallel spins.

The tradeoff bound for parallel spins has already obtained in [24]:

$$\mathcal{I}_{\text{para}} = \tfrac{1}{9}(6 - \mathcal{D} + \sqrt{2\mathcal{D}(3 - 4\mathcal{D})}). \tag{38}$$

Compared with parallel spins, antiparallel spins contain a much higher amount of information for the same disturbance $\mathcal{D}$:

$$\mathcal{I}_{\text{anti}} \geqslant \mathcal{I}_{\text{para}}, \tag{39}$$

where the equality holds only in the case of minimal disturbance measurement: $\mathcal{D} = 0$. For ease, a comparative plot of the information–disturbance tradeoff between the case of the antiparallel spin and the case of the parallel spin is given in figure 2(a). Moreover, we also plot the amount of enhancement $\Delta\mathcal{I}/\mathcal{I}_{\text{para}} = (\mathcal{I}_{\text{anti}} - \mathcal{I}_{\text{para}})/\mathcal{I}_{\text{para}}$ as a function of disturbance $\mathcal{D}$. Numerical analysis reveals that the maximal value of $\Delta\mathcal{I}$ can be up to 5.470% at $\mathcal{D} = 0.147$.

Via antiparallel spins, Alice gains a definite improvement in her transmission of direction information. A more powerful and physically available measurement exists to obtain much more information than the case of parallel spins. However, this is not complete, particularly if we keep the security of direction information in mind. Suppose an eavesdroppers Eve is tapping the quantum channel. It is she (not Bob) who performs the optimal quantum measurement on the antiparallel spins. Then after observing the measurement outcome r, the disturbed state is then sent to the legal receiver, Bob. It is not enough to remove all of Eve's tapped information simply by checking the average disturbance $\mathcal{D}$ and by performing the privacy amplification protocol [30] for parallel spins. Antiparallel spins improve Eve's information too. She could obtain a higher amount of information for the same disturbance. This means that a higher amount of information should be distilled out if we want to keep the direction information secure.

6. Conclusions

In this paper, a strict information–disturbance bound for antiparallel spins, along with the optimal POVM measurement which attains the bound is obtained. Such a result can be of practical relevance since it imposes a general limit on Eve's information extraction and her disturbance on the quantum spins. Finally, we give a comparison between the tradeoff in antiparallel and parallel cases, which reveals that a higher amount of information should be distilled out if we use the antiparallel spin for secure transmission of direction information.

Acknowledgments

This work was supported by National Fundamental Research Program, also by National Natural Science Foundation of China (grant no 10674128 and 60121503) and the Innovation Funds and 'Hundreds of Talents' program of Chinese Academy of Sciences and Doctor Foundation of Education Ministry of China (grant no 20060358043).

References

[1] Bartlett S, Rudolph T and Spekkens R 2007 Reference frames, superselection rules, and quantum information *Rev. Mod. Phys.* **79** 555

[2] Peres A and Petra S F 2002 Unspeakable quantum information arXiv:quant-ph/0201017

[3] Peres A and Wootters K W 1991 Optimal detection of quantum information *Phys. Rev. Lett.* **66** 1119

[4] Bagan E, Baig M and Muñoz-Tapia R 2001 Aligning reference frames with quantum states *Phys. Rev. Lett.* **87** 257903

[5] Bagan E, Baig M, Brey A, Muñoz-Tapia R and Tarrach R 2000 Optimal strategies for sending information through a quantum channel *Phys. Rev. Lett.* **85** 5230

[6] Chiribella G, D'Ariano G M, Perinotti P and Sacchi M F 2004 Efficient use of quantum resources for the transmission of a reference frame *Phys. Rev. Lett.* **93** 180503

[7] Peres A and Petra S F 2001 Transmission of a Cartesian frame by a quantum system *Phys. Rev. Lett.* **87** 167901

[8] Peres A and Petra S F 2001 Entangled quantum states as direction indicators *Phys. Rev. Lett.* **86** 4160

[9] Massar S and Popescu S 1995 Optimal extraction of information from finite quantum ensembles *Phys. Rev. Lett.* **74** 1259

[10] Gisin N and Popescu S 1999 Spin flips and quantum information for antiparallel spins *Phys. Rev. Lett.* **83** 432

[11] Massar S 2000 Collective versus local measurements on two parallel or antiparallel spins *Phys. Rev.* A **62** 040101

[12] Kolenderski P and Demkowicz-Dobrzanski R 2008 Optimal state for keeping reference frames aligned and the platonic solids *Phys. Rev.* A **78** 052333

[13] Chiribella G, Maccone L and Perinotti P 2007 Secret quantum communication of a reference frame *Phys. Rev. Lett.* **98** 120501

[14] Fuchs C A and Peres A 1996 Quantum-state disturbance versus information gain: uncertainty relations for quantum information *Phys. Rev.* A **53** 2038

[15] Fuchs C A and Jacobs K 2001 Information-tradeoff relations for finite-strength quantum measurements *Phys. Rev.* A **63** 062305

[16] Mišta L, Fiurášek J and Filip R 2005 Optimal partial estimation of multiple phases *Phys. Rev. A* **72** 012311

[17] Maccone L 2006 Information-disturbance tradeoff in quantum measurements *Phys. Rev.* A **73** 042307

[18] Buscemi F and Sacchi M F 2006 Information-disturbance trade off in quantum-state discrimination *Phys. Rev.* A **74** 052320

[19] Banaszek K 2001 Fidelity balance in quantum operations *Phys. Rev. Lett.* **86** 1366

[20] Banaszek K and Devetak I 2001 Fidelity trade off for finite ensembles of identically prepared qubits *Phys. Rev.* A **64** 052307

[21] Sacchi M F 2006 Information-disturbance tradeoff in estimating a maximally entangled state *Phys. Rev. Lett.* **96** 220502

[22] Davies E B 1978 Information and quantum measurement *IEEE Trans. Inf. Theory* **24** 596

[23] Kraus K 1983 *States, Effects, and Operations* (Berlin: Springer)

[24] Mišta L and Fiurášek J 2006 Optimal partial estimation of quantum states from several copies *Phys. Rev.* A **74** 022316

[25] Demkowicz-Dobrzański R, Lewenstein M, Sen(De) A, Sen U and Bruß D 2006 Usefulness of classical communication for local cloning of entangled states *Phys. Rev.* A **73** 032313

[26] Novotný J, Alber G and Jex I 2005 Optimal copying of entangled two-qubit states *Phys. Rev.* A **71** 042332

[27] Chiribella G, D'Ariano G M and Perinotti P 2005 Extremal quantum cloning machines *Phys. Rev.* A **72** 042336

[28] D'Ariano G M and Sacchi M F 2005 Optimal estimation of group transformations using entanglement *Phys. Rev.* A **72** 042338

[29] Zhelobenko D P 1973 *Compact Lie Groups and Their Representations* (Providence, RI: American Mathematical Society)

[30] Deutsch D, Ekert A, Jozsa R, Macchiavello C, Popescu S and Sanpera A 1996 Quantum privacy amplification and the security of quantum cryptography over noisy channels *Phys. Rev. Lett.* **77** 2818