Int J Theor Phys (2009) 48: 3353–3357
DOI 10.1007/s10773-009-0138-3

Establishing a Private Shared Reference Frame via the Distillation of Entanglement

Koji Nagata

Received: 7 May 2009 / Accepted: 2 September 2009 / Published online: 16 September 2009

Abstract We show how a collection of N ebits can be used to establish a private shared reference frame, in the sense that a relative orientation of the x and y axes with respect to a publicly-known z axis is unconditionally private to Alice and Bob. Our protocol relies on the distillation protocol of entanglement. The scheme is based on tensor product states of spin pairs. We implicitly assume a shared reference frame (which is not guaranteed to be private) at the beginning of the protocol. It turns out that the entanglement distillation protocol implies the construction of a private shared reference frame.

Keywords Entalgement protocol · Quantum information theory

1 Introduction

How to establish a shared reference frame (SRF) between the sender (Alice) and receiver (Bob) has been researched. It is important because Alice and Bob need a SRF when they do practical realizations of quantum information processes [1, 2]. Several researches address the problem in Refs. [3–11]. It is discussed that SRF can be quantified as refbits in Ref. [12]. (See also Ref. [13].)

It is desirable that an eavesdropper (Eve) does not know a relative orientation of a SRF when Alice and Bob do quantum cryptography since Eve's information about communication between them is restricted as discussed in Ref. [14]. However, it has not been explicitly discussed in the literature how to establish such a private SRF till now. Suppose that Alice and Bob do quantum cryptography when they are far away from each other. A relative orientation of Cartesian frame may be determined using fixed stars and gyroscopes. But, Eve can know a relative orientation when she knows their strategy. Therefore the problem is raised in Ref. [14]. Namely, how is a private SRF established?

In this paper, we propose how to establish a private SRF. Let us explain our scheme briefly. First, Alice and Bob share a public SRF. Next, they perform the entanglement distillation protocol in Ref. [15]. Thereby, they can share many singlet states (EPR pairs). Finally,

K. Nagata (✉)
Obihiro University of Agriculture and Veterinary Medicine, Obihiro, Japan
e-mail: ko_mi_na1@yahoo.co.jp

they perform a protocol proposed in this paper. Here, one can see new property of the distillation of entanglement.

The final protocol is as follows: Assume that Alice and Bob share a set of N EPR pairs (N ebits). In the set, Alice does separable measurements of Pauli observable σ_x on each of the N EPR pairs and sends outcomes (± 1) to Bob, (they are N bits), by using classical communication. Bob performs local operation on the corresponding qubit in his side if the corresponding outcome is $+1$. Then Bob does a single square root measurement on all his N qubits. Finally, Bob evaluates measurement outcome.

We use such measurements since it is discussed that the positive operator valued measures (POVMs) are optimal in Refs. [16, 17] in order to estimate a single parameter, in the sense that a specific score is maximized. Such a score is something like that

$$\sum (\text{Probability of a situation}) \times (\text{Fidelity to an ideal situation}). \tag{1}$$

Here, the summation is taken over all possible situations.

2 Protocol via Distillation of Entanglement

It is easy to imagine that Alice and Bob construct a public SRF. Let us start from an assumption. The assumption is that there are many distillable entangled pairs of qubits. Here, each pair of qubits is described by an identical state ρ. Then, the assumption mentioned above is satisfied if $\langle \Psi_{\mathrm{EPR}}|\rho|\Psi_{\mathrm{EPR}}\rangle > 1/2$. Here, $|\Psi_{\mathrm{EPR}}\rangle = \frac{1}{\sqrt{2}}(|1^a 0^b\rangle - |0^a 1^b\rangle)$. The state ρ is, necessarily, an (noisy) entangled state. Alice and Bob perform the distillation protocol described in Ref. [15] many times. Thereby, Alice and Bob share many EPR pairs.

In what follows, we imagine a set of N EPR pairs. First, Alice rotates her Cartesian frame with respect to the z axis by an angle θ_n in secretly against Eve. The angle is constrained to the values:

$$\theta_n = \frac{2\pi n}{N+1} \quad (n = 0, 1, \ldots, N). \tag{2}$$

Imagine she uses N EPR pairs. She performs separable measurements on her side of the state of $|\Psi_{\mathrm{EPR}}\rangle^{\otimes N}$. We assume that the separable measurement is described by Pauli operator $\sigma_x^a = |1^a\rangle\langle 0^a| + |0^a\rangle\langle 1^a|$ in the orientation of Cartesian frame at Alice side. Then, Bob immediately gets the tensor product of the following state in the orientation of Cartesian frame at Bob side:

$$\begin{aligned} |\psi_{\theta_n}^-\rangle &= \frac{1}{\sqrt{2}}(|0^b\rangle + e^{-i\theta_n}|1^b\rangle), \\ |\psi_{\theta_n}^+\rangle &= \frac{1}{\sqrt{2}}(|0^b\rangle - e^{-i\theta_n}|1^b\rangle). \end{aligned} \tag{3}$$

Bob wants to know the integer n that represents Alice's x-direction. Alice sends the outcome (± 1) to Bob. Please note this classical communication does not give Eve any information about n since it should be random bits. When the outcome is $+1$, Bob performs local operation $-\sigma_z^b$ to his state as follows:

$$\begin{aligned} -\sigma_z^b|\psi_{\theta_n}^+\rangle &= -\sigma_z^b \frac{1}{\sqrt{2}}(|0^b\rangle - e^{-i\theta_n}|1^b\rangle) \\ &= \frac{1}{\sqrt{2}}(|0^b\rangle + e^{-i\theta_n}|1^b\rangle) \end{aligned} \tag{4}$$

where

$$-\sigma_z^b = |0^b\rangle\langle 0^b| - |1^b\rangle\langle 1^b|. \tag{5}$$

Thereby, Bob gets the state $|\psi_{\theta_n}^-\rangle^{\otimes N}$. Let us define $|\Psi_{\theta_n}\rangle$ as $|\psi_{\theta_n}^-\rangle^{\otimes N}$. Please note that $|\Psi_{\theta_n}\rangle$ is rewritten as follows (cf. [16]):

$$|\Psi_{\theta_n}\rangle = \sum_{\vec{n}} \frac{\sqrt{N!}}{\sqrt{n_0!}\sqrt{n_1!}} \left(\frac{1}{\sqrt{2}}\right)^{n_0} \left(\frac{1}{\sqrt{2}}\right)^{n_1} e^{-i\theta_n n_1} |\vec{n}\rangle, \tag{6}$$

where $\sum_{\vec{n}}$ means the summation over two-tuples $\vec{n} = (n_0, n_1)$ with $n_0 + n_1 = N$, and $|\vec{n}\rangle (\equiv |(n_0, n_1)\rangle)$ is the occupation number basis. We introduce $A(\vec{n})$ as

$$A(\vec{n}) = \frac{\sqrt{N!}}{\sqrt{n_0!}\sqrt{n_1!}} \left(\frac{1}{\sqrt{2}}\right)^{n_0} \left(\frac{1}{\sqrt{2}}\right)^{n_1}, \tag{7}$$

then we have

$$|\Psi_{\theta_n}\rangle = \sum_{\vec{n}} A(\vec{n}) e^{-i\theta_n n_1} |\vec{n}\rangle. \tag{8}$$

Now, Bob's task is to estimate the integer n by measuring the state (8). He performs a single square root measurement on $|\Psi_{\theta_n}\rangle$. It is shown [16] that such a measurement is optimal to estimate a single parameter θ_n, in the sense that a specific score be maximized as mentioned above. We derive POVMs as in Ref. [16]. Bob introduces the following $N + 1$ states:

$$|\psi_m\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{-i(\frac{2\pi m}{N+1})}|1\rangle) \quad (m = 0, 1, \ldots, N). \tag{9}$$

Let us define $|\Psi_m\rangle$ as $|\psi_m\rangle^{\otimes N}$. Then we have

$$|\Psi_m\rangle = \sum_{\vec{n}} A(\vec{n}) e^{-i(\frac{2\pi m}{N+1})n_1} |\vec{n}\rangle. \tag{10}$$

The POVMs $\{|\mu_m\rangle\}$ is described as follows:

$$|\mu_m\rangle = \hat{\Psi}^{-1/2}|\Psi_m\rangle, \quad \hat{\Psi} = \sum_{m=0}^{N} |\Psi_m\rangle\langle\Psi_m|. \tag{11}$$

$\hat{\Psi}$ is calculated as follows:

$$\begin{aligned}
\hat{\Psi} &= \sum_{m=0}^{N} |\Psi_m\rangle\langle\Psi_m| \\
&= \sum_{m=0}^{N} \left(\sum_{\vec{n}} A(\vec{n}) e^{-i(\frac{2\pi m}{N+1}n_1)} |\vec{n}\rangle \sum_{\vec{n}'} A(\vec{n}') e^{-i(\frac{2\pi m}{N+1}n_1')} \langle\vec{n}'| \right) \\
&= \sum_{\vec{n}} \sum_{\vec{n}'} A(\vec{n}) A(\vec{n}') \sum_{m=0}^{N} e^{-i(\frac{2\pi m}{N+1})(n_1 - n_1')} |\vec{n}\rangle\langle\vec{n}'|
\end{aligned}$$

$$= (N+1)\sum_{\vec{n}}\sum_{\vec{n}'} A(\vec{n})A(\vec{n}')\delta_{n_1,n_1'}|\vec{n}\rangle\langle\vec{n}'|$$
$$= (N+1)\sum_{\vec{n}} A(\vec{n})^2|\vec{n}\rangle\langle\vec{n}|. \tag{12}$$

Hence, $\hat{\Psi}^{-1/2}$ is

$$\hat{\Psi}^{-1/2} = \frac{1}{\sqrt{N+1}}\sum_{\vec{n}}{}' \frac{1}{A(\vec{n})}|\vec{n}\rangle\langle\vec{n}|. \tag{13}$$

Therefore, we obtain the POVMs as follows:

$$\begin{aligned}|\mu_m\rangle &= \hat{\Psi}^{-1/2}|\Psi_m\rangle \\ &= \frac{1}{\sqrt{N+1}}\sum_{\vec{n}}\frac{1}{A(\vec{n})}|\vec{n}\rangle\langle\vec{n}|\sum_{\vec{n}'}A(\vec{n}')e^{-i(\frac{2\pi m}{N+1})n_1'}|\vec{n}'\rangle \\ &= \frac{1}{\sqrt{N+1}}\sum_{\vec{n}} e^{-i(\frac{2\pi m}{N+1})n_1}|\vec{n}\rangle. \end{aligned}\tag{14}$$

It is worth mentioning that the algebra written above agrees with the result obtained in Ref. [17]. Since $\langle\mu_m|\mu_{m'}\rangle = \delta_{m,m'}$, the measurement is reduced to von Neumann measurement. Bob performs measurement on the state (8) by using the POVMs $\{|\mu_m\rangle\}$. Then, Bob obtains measurement outcome with respect to the specific subscript m. He estimates the integer m by using the following scheme. In this scheme, m should be as $m = n$ in the maximal probability as shown below. First, we have

$$\begin{aligned}\langle\Psi_{\theta_n}|\mu_m\rangle &= \sum_{\vec{n}} A(\vec{n})e^{i\theta_n n_1}\langle\vec{n}|\frac{1}{\sqrt{N+1}}\sum_{\vec{n}'}e^{-i(\frac{2\pi m}{N+1})n_1'}|\vec{n}'\rangle \\ &= \frac{1}{\sqrt{N+1}}\sum_{\vec{n}} A(\vec{n})e^{-i(\frac{2\pi(m-n)}{N+1})n_1}. \end{aligned}\tag{15}$$

Therefore, for the measurement probability $|\langle\Psi_{\theta_n}|\mu_m\rangle|^2$ of each of m, we have

$$\begin{aligned}|\langle\Psi_{\theta_n}|\mu_m\rangle|^2 &= \frac{1}{N+1}\sum_{\vec{n}}\sum_{\vec{n}'}A(\vec{n})A(\vec{n}')e^{-i(\frac{2\pi(m-n)}{N+1})(n_1-n_1')} \\ &= \frac{1}{N+1}\sum_{\vec{n}}\sum_{\vec{n}'}A(\vec{n})A(\vec{n}')\cos\left(\left(\frac{2\pi(m-n)}{N+1}\right)(n_1-n_1')\right) \\ &\le \frac{1}{N+1}\sum_{\vec{n}}\sum_{\vec{n}'}A(\vec{n})A(\vec{n}'). \end{aligned}\tag{16}$$

The equality of the relation (16) holds when $m = n$. Hence, m should be estimated as $m = n$ in the maximal probability. The question how Bob actually estimates the integer m is open problem. Bell inequalities in Refs. [18, 19] gives a clue.

We summarize our protocol:

1. Alice and Bob share a public SRF.
2. Alice and Bob perform the entanglement distillation protocol.
3. Alice and Bob share many EPR pairs.
4. Alice rotates her Cartesian frame with respect to the z axis (cf. (2)).
5. Alice performs separable measurement on a set of EPR pairs on her side.
6. Alice sends a set of measurement outcome (random bits).
7. Bob performs local operations on states on his side if necessary (cf. (4)).
8. Bob performs a single square root measurement on his state (8).
9. Bob gets a measurement result.
10. Bob rotates his Cartesian frame according to measurement result with respect to the z axis.
11. Probability of desirable result is maximal.

3 Summary

In summary, we have shown that the entanglement distillation protocol implies the construction of a private shared reference frame. Our argument revealed new relation between the entanglement distillation and a private shared reference frame.

Acknowledgements The author thanks M. Takeoka, J.A. Vaccaro, and M. Sasaki for valuable discussions.

References

1. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2000)
2. Peres, A.: Quantum Theory: Concepts and Methods. Kluwer Academic, Dordrecht (1993)
3. Massar, S., Popescu, S.: Phys. Rev. Lett. **74**, 1259 (1995)
4. Gisin, N., Popescu, S.: Phys. Rev. Lett. **83**, 432 (1999)
5. Peres, A., Scudo, P.F.: Phys. Rev. Lett. **86**, 4160 (2001)
6. Peres, A., Scudo, P.F.: Phys. Rev. Lett. **87**, 167901 (2001)
7. Bagan, E., Baig, M., Munoz-Tapia, R.: Phys. Rev. Lett. **87**, 257903 (2001)
8. Acin, A., Jane, E., Vidal, G.: Phys. Rev. A **64**, 050302(R) (2001)
9. Lindner, N.H., Peres, A., Terno, D.R.: Phys. Rev. A **68**, 042308 (2003)
10. Chiribella, G., D'Ariano, G.M., Perinotti, P., Sacchi, M.F.: Phys. Rev. Lett. **93**, 180503 (2004)
11. Bagan, E., Baig, M., Munoz-Tapia, R.: Phys. Rev. A **70**, 030301(R) (2004)
12. van Enk, S.J.: Phys. Rev. A **71**, 032339 (2005)
13. Vaccaro, J.A., Anselmi, F., Wiseman, H.M., Jacobs, K.: arXiv:quant-ph/0501121
14. Bartlett, S.D., Rudolph, T., Spekkens, R.W.: Phys. Rev. A **70**, 032307 (2004)
15. Bennett, C.H., Brassard, G., Popescu, S., Schumacher, B., Smolin, J.A., Wootters, W.K.: Phys. Rev. Lett. **76**, 722 (1996)
16. Sasaki, M., Carlini, A., Chefles, A.: J. Phys. A: Math. Gen. **34**, 7017 (2001)
17. Derka, R., Buzek, V., Ekert, A.K.: Phys. Rev. Lett. **80**, 1571 (1998)
18. Bramon, A., Nowakowski, M.: Phys. Rev. Lett. **83**, 1 (1999)
19. Ancochea, B., Bramon, A., Nowakowski, M.: Phys. Rev. D **60**, 094008 (1999)