Quantum Information and Computation, Vol. 5, No. 7 (2005) 605–606

ERRATUM

to

QUANTUM AND CLASSICAL MESSAGE IDENTIFICATION VIA QUANTUM CHANNELS

ANDREAS WINTER
School of Mathematics, University of Bristol
University Walk, Bristol BS8 1TW, U.K.
Email: a.j.winter@bris.ac.uk

Received August 5, 2005

The article, Ref. 1, by the author has several crucial oversights and mathematical errors in the proof of Proposition 16. This concerns the argument from the top of p. 574 to the end of the proof, a corrected version of which is offered here. The statement of Proposition 16 remains unchanged. It should be noted that Ref. 1 is a verbatim reprint of Ref. 2, except for a changed numbering scheme of the sequence of Propositions, Lemmas, etc.: the same errors and correction apply to Ref. 2, there in the proof of Proposition 17, from the middle of p. 184 (the big display equation).

Proof of Proposition 16 (Proposition 17 in Ref. 2).
... constant for the moment, so that $D_\tau = \operatorname{supp} \operatorname{Tr}_a |v\rangle\langle v|$ is a constant, we have

$$\begin{aligned}
\operatorname{Tr}(\varepsilon(\pi)D_\tau) &= \langle\phi|V^*(D_\tau \otimes \mathbb{1})V|\phi\rangle \\
&= \left(\left(\sqrt{\alpha} - \sqrt{1-\alpha}\frac{\langle w|v\rangle}{t}\right)\langle v| + \frac{\sqrt{1-\alpha}}{t}\langle w|\right) \\
&\qquad D_\tau \otimes \mathbb{1} \; \left(\left(\sqrt{\alpha} - \sqrt{1-\alpha}\frac{\langle v|w\rangle}{t}\right)|v\rangle + \frac{\sqrt{1-\alpha}}{t}|w\rangle\right) \\
&= \left|\sqrt{\alpha} - \sqrt{1-\alpha}\frac{\langle v|w\rangle}{t}\right|^2 + \frac{1-\alpha}{t^2}\langle w|D_\tau \otimes \mathbb{1}|w\rangle \\
&\quad + \left(\sqrt{\alpha} - \sqrt{1-\alpha}\frac{\langle w|v\rangle}{t}\right)\frac{\sqrt{1-\alpha}}{t}\langle v|w\rangle \\
&\quad + \left(\sqrt{\alpha} - \sqrt{1-\alpha}\frac{\langle v|w\rangle}{t}\right)\frac{\sqrt{1-\alpha}}{t}\langle w|v\rangle \\
&= \alpha + \frac{1-\alpha}{t^2}\big[\langle w|D_\tau \otimes \mathbb{1}|w\rangle - \langle w|v\rangle\langle v|w\rangle\big],
\end{aligned}$$

where we have denoted $t := \| |w\rangle - \langle v|w\rangle |v\rangle \|_2$ and used that $|v\rangle\langle v| \leq D_\tau \otimes \mathbb{1}$. Hence, if

$$\langle w|v\rangle\langle v|w\rangle \leq \langle w|D_\tau \otimes \mathbb{1}|w\rangle \stackrel{!}{\leq} \epsilon := (\eta/2)^2, \tag{13}$$

we can conclude that $\left|\mathrm{Tr}\varepsilon(\pi)D_\tau - \alpha\right| \leq \eta$. It remains to bound the probability of the event in eq. (13): according to Lemma 2 (Lemma 18 in Ref. 2), putting $a = \lfloor \epsilon d/2 \rfloor$, we have

$$\Pr\{\langle w|D_\tau \otimes \mathbb{1}|w\rangle > \epsilon\} \leq \exp\left(-a^2 \frac{1 - \ln 2}{\ln 2}\right).$$

Note that D_τ can have rank a at most; we will assume $a \geq 1$ from now, and will see at the end that the case where a would be zero is trivial. Putting this and eq. (13) together with the union bound, this gives us

$$\begin{aligned}
\Pr\Big\{\exists\pi,\tau \text{ from the } \eta\text{–net } \left|\mathrm{Tr}\varepsilon(\pi)D_\tau - \mathrm{Tr}\pi\tau\right| > \eta\Big\} &\leq \left(\frac{5}{\eta}\right)^{4S} \exp\left(-\frac{1 - \ln 2}{\ln 2}\left\lfloor\frac{\epsilon d}{2}\right\rfloor^2\right) \\
&\leq \left(\frac{40}{\lambda}\right)^{4S} \exp\left(-\frac{1 - \ln 2}{16 \ln 2}(\lambda/16)^4 d^2\right),
\end{aligned}$$

which is smaller than 1 by our choice of parameters: $\eta = \lambda/8$, $\epsilon = (\eta/2)^2$, $S = \left\lfloor d^2 \frac{(\lambda/100)^4}{4 \log(100/\lambda)} \right\rfloor$. That is, except when $S = 0$ (which is implied by $a = 0$), in which case the proposition is trivial. □

References

1. A. Winter, "Quantum and Classical Message Identification Via Quantum Channels", *Quantum Inf. Comput.*, **4**(6&7), 563–578 (2004).
2. A. Winter, "Quantum and Classical Message Identification Via Quantum Channels", in: *Quantum Information, Statistics, Probability: Dedicated to Alexander S. Holevo on the occasion of his 60th birthday*, O. Hirota (ed.), 172–190, Rinton Press, Princeton NJ (2004).