September 1, 2016 (Thursday)

[

Spin-based quantum computing in a silicon CMOS-compatible platform

Andrew S. Dzurak

UNSW, School of Electrical Engineering, Sydney, Australia

Abstract. Spin qubits in silicon are excellent candidates for scalable quantum information processing [1] due to their long coherence times and the enormous investment in silicon CMOS technology. While our Australian effort in Si QC has largely focused on spin qubits based upon phosphorus dopant atoms implanted in Si [2,3], we are also exploring spin qubits based on single electrons confined in SiMOS quantum dots [4]. Such qubits can have long spin lifetimes T1=2 s, while electric field tuning of the conduction-band valley splitting removes problems due to spin-valley mixing [5]. In isotopically enriched Si-28 these SiMOS qubits have a control fidelity of 99.6% [6], consistent with that required for fault-tolerant QC. By gate-voltage tuning the electron g∗-factor, the ESR operation frequency can be Stark shifted by > 10 MHz [6], allowing individual addressability of many qubits. Most recently we have coupled two SiMOS qubits to realize CNOT gates [7] for which over 25 gates can be performed within a two-qubit coherence time of 8 μs. I will conclude by discussing the prospects of scalability of this technology using traditional CMOS manufacturing.

]

References

[1] D.D. Awschalom et al., "Quantum Spintronics", Science 339, 1174 (2013).

[2] J.J. Pla et al., "A single-atom electron spin qubit in silicon", Nature 489, 541 (2012).

[3] J.T. Muhonen et al., "Storing quantum information for 30 seconds in a nanoelectronic device", Nature Nanotechnology 9, 986 (2014).

[4] S.J. Angus et al., "Gate-defined quantum dots in intrinsic silicon", Nano Lett. 7, 2051 (2007).

[5] C.H. Yang et al., "Spin-valley lifetimes in a silicon quantum dot with tunable valley splitting", Nature Comm. 4, 2069 (2013).

[6] M. Veldhorst et al., "An addressable quantum dot qubit with fault-tolerant control fidelity", Nature Nanotechnology 9, 981 (2014).

[7] M. Veldhorst et al., "A two-qubit logic gate in silicon", Nature 526, 410 (2015).

Storage of multiple single-photon pulses emitted from a quantum dot in a solid-state quantum memory

Jian-Shun Tang[1 2 *] Zong-Quan Zhou[1 2] Chuan-Feng Li[1 2 †] Guang-Can Guo [1 2]

[1] *Key Laboratory of Quantum Information, University of Science and Technology of China, CAS, Hefei, Anhui 230026, China.*

[2] *Synergetic Innovation Center of Quantum Information & Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China.*

Abstract. Quantum repeaters are critical components for distributing entanglement over long distances in presence of unavoidable optical losses during transmission. Stimulated by Duan-Lukin-Cirac-Zoller protocol, many improved quantum-repeater protocols based on quantum memories have been proposed, which commonly focus on the entanglement-distribution rate. Among these protocols, the elimination of multiple photons (or multiple photon-pairs) and the use of multimode quantum memory are demonstrated to have the ability to greatly improve the entanglement-distribution rate. Here, we demonstrate the storage of deterministic single photons emitted from a quantum dot in a polarization-maintaining solid-state quantum memory; in addition, multi-temporal-mode memory with 1, 20 and 100 narrow single-photon pulses is also demonstrated. Multi-photons are eliminated, and only one photon at most is contained in each pulse. Moreover, the solid-state properties of both sub-systems make this configuration more stable and easier to be scalable. Our work will be helpful in the construction of efficient quantum repeaters based on all-solid-state devices.

Keywords: deterministic single photon, multiple temporal modes, quantum memory

1 Introduction

Long-distance entanglement distribution has become increasingly important, which is essential in the improvement of many quantum technologies, such as quantum key distribution [1] and quantum internet [2]. It is also helpful in the examination of the foundation problems in quantum mechanics, for example, the Bell-inequality test [3]. However, this task is not easy to perform, because of the photon loss during the fiber transmission. One proposal to overcome this issue is to use quantum repeaters [4]. In this architecture, the entire distance is divided into several shorter elementary links, and for each link, entanglement between quantum memories can be established independently. Next, the elementary links are joined using entanglement swapping to create an entangled pair over the entire distance. The storage of the deterministic single photons and especially their storage in a multimode configuration is very critical in the construction of a high-efficiency quantum repeater.

In this work we experimentally demonstrate two points (details are shown in Ref. [6]). The first point is the storage of deterministic single photons (with no multi-photons in principle) emitted from a semiconductor self-assembled quantum dot (QD) in a solid-state polarization-maintaining quantum memory [7], which is based on Nd^{3+}:YVO_4 crystals. The QD and the Rare-earth (RE)-ion-doped crystals are separated by 5 m on two separate optical tables and are connected via a 10-m fiber. The second point is the realization of the temporal multiplexed quantum memory with QD-based narrow single-photon pulses. 1, 20 and 100 temporal modes are respectively stored in the quantum memory, with at most one photon present in each mode. Both of these points will be helpful in the development of quantum repeaters. Moreover, both sub-systems in our experiment are solid-state, which will make this configuration more stable and convenient.

2 Results

Storage of multiple single-photon pulses. We use an electro-optic modulator (EOM) to chop the excitation laser for the QD. The pulsewidth of the excitation laser $T_{\mathrm{expw}} = 0.8$ ns is reduced to be less than the QD's lifetime, which ensures there is only one photon in a single pulse. This point is also demonstrated by the Hanbury Brown-Twiss experiment ($g^{(2)}(0) = 0.14$).

Figure 1(a) shows the result of the storage for 1 single-photon pulse with $T_{\mathrm{period}} = 400$ ns and $T_{\mathrm{storage}} = 40$ ns. The integration time is 11.7 hours. The peak at 0 ns corresponds to the single photons that are not absorbed without wetting-layer light, the peak at 40 ns corresponds to the single photons that are stored, and the peak at 80 ns is the second-order retrieved single photons. Two sets of filter and etalon (with a different free spectral range (FSR)) are inserted in the beampath here to filter the single photons more clearly. In this situation, the second peak is almost as high as the first peak. In Figure 1(b), 20 single-photon pulse are stored in the quantum memory with $T_{\mathrm{period}} = 400$ ns and $T_{\mathrm{storage}} = 100$ ns. The integration time is 7.5 hours, and the separation between the neighboring modes is 4.8 ns. 20 peaks are clearly seen in the range of $100 \sim 200$ ns, which are the stored single-photon temporal modes. The peaks in the ranges of $0 \sim 100$ ns and $200 \sim 300$ ns are the transmitted light and the second-order retrieved light, respectively.

*tjs@ustc.edu.cn

†cfli@ustc.edu.cn

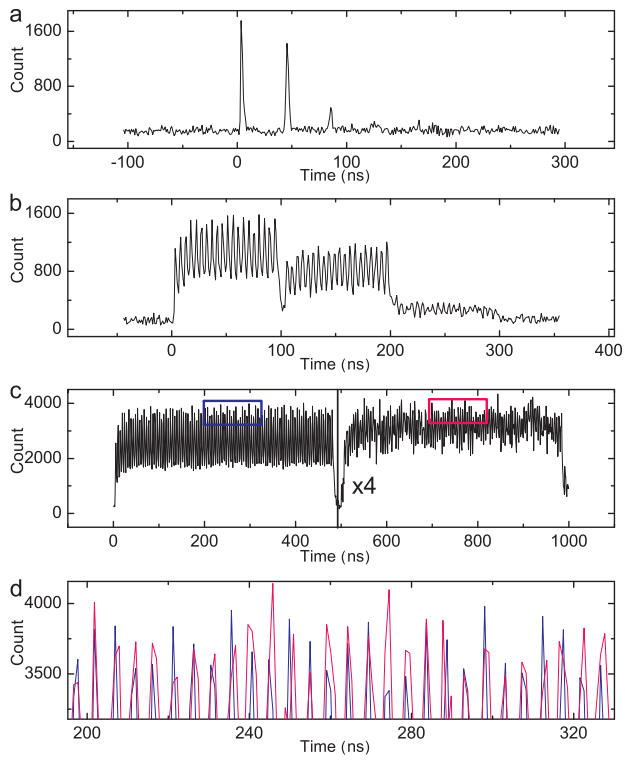


Figure 1: **The quantum storage of multiple single-photon pulses.** We use an EOM to modulate the excitation light here, and its pulsewidth T_{expw} is reduced to 0.8 ns, which ensures there is at most one photon in each pulse. (a) 1, (b) 20 and (c) 100 temporal modes of the single photons are used for the quantum memory. (d) The enlargement of the rectangle-regions in (c). This result shows that the temporal modes of the single photons are well maintained during the memory process.

We also examine the situation of 100 modes with $T_{\mathrm{period}} = 1000$ ns and $T_{\mathrm{storage}} = 500$ ns, as shown in Figure 1(c). The integration time and the separation between the neighboring modes are 46.1 hours and 4.8 ns, respectively. The peaks in the ranges of $0 \sim 500$ ns and $500 \sim 1000$ ns are the transmitted light and the retrieved single photons, respectively. In fact, the efficiency of quantum memory is related to the storage time. In the present situation, the efficiency is approximately 7%, whereas this value is estimated to be 20% and 13% in the situations of $T_{\mathrm{storage}} = 40$ ns and $T_{\mathrm{storage}} = 100$ ns, respectively. In spite of the decrease of the memory efficiency, we can still clearly observe 100 small peaks from the retrieved photons. Figure 1(d) shows the details of the peaks in the blue rectangle of Figure 1(c) and those in the pink rectangle with the time-coordinate subtracted by $T_{\mathrm{storage}} = 500$ ns. Each of these peaks corresponds well to each other one by one. This phenomenon shows the reliability of our experimental results.

3 Discussion

Our work is the first demonstration of the storage of the QD-based deterministic-single-photon pulse trains. Both the sub-quantum systems in this configuration, namely, the QD and the RE-ion-doped crystals, are solid-state materials. Moreover, we demonstrate that the polarization states of the single photons can be well preserved. Therefore, both the polarization states and the time bins can be used to encode the qubits. One possible application of our configuration is the quantum repeater protocol recently proposed by Sinclair *et al.* [8], which is based on spectral multiplexing, multimode AFC delay quantum memory, entangled photon-pair sources, Bell-state measurement and feed-forward control. Another example of the application of our configuration is the quantum repeater protocol based on single photon sources [5], which improves upon the Duan-Lukin-Cirac-Zoller (DLCZ) protocol by replacing the photon-pair sources (an equivalent protocol as the DLCZ one) with the single photon sources.

To conclude, we achieve the storage of deterministic single photons emitted from a QD in a sandwich-like Nd^{3+}:YVO_4 quantum memory, which can preserve the polarization states of the input photons. We have also demonstrated the temporal multimode operation of the quantum memory with 1, 20 and 100 narrow single-photon pulses. Only one photon exists in a single pulse at most. Our work paves the way toward the construction of high-speed quantum repeaters based on all-solid-state devices and can also be used in other quantum technologies.

References

[1] N. Gisin, G. Ribordy, W. Tittel & H. Zbinden. Quantum cryptography. *Rev. Mod. Phys.* **74**:145-195, 2002.

[2] H. J. Kimble. The quantum internet. *Nature* **453**:1023-1030, 2008.

[3] J. S. Bell. On the Einstein Podolsky Rosen paradox. *Physics* **1**:195-200, 1964.

[4] H.-J. Briegel, W. Dür, J. I. Cirac & P. Zoller. Quantum repeaters: The role of imperfect local operations in quantum communication. *Phys. Rev. Lett.* **81**:5932-5935, 1998.

[5] N. Sangouard *et al.* Long-distance entanglement distribution with single-photon sources. *Phys. Rev. A* **76**:050301(R), 2007.

[6] J.-S. Tang *et al.* Storage of multiple single-photon pulses emitted from a quantum dot in a solid-state quantum memory. *Nature Communications* **6**:8652, 2015.

[7] Z.-Q. Zhou, W.-B. Lin, M. Yang, C.-F. Li & G.-C. Guo. Realization of reliable solid-state quantum memory for photonic polarization qubit. *Phys. Rev. Lett.* **108**:190505, 2012.

[8] N. Sinclair *et al.* Spectral multiplexing for scalable quantum photonics using an atomic frequency comb quantum memory and feed-forward control. *Phys. Rev. Lett.* **113**:053603, 2014.

Experimentally Secure Relativistic Bit Commitment

Matej Pivoluska,[1,2] Marcin Pawłowski,[3] and Martin Plesch[2,1]

[1] *Faculty of Informatics, Masaryk University, Botanická 68a, 602 00 Brno, Czech Republic*
[2] *Institute of Physics, Slovak Academy of Sciences, Bratislava, Slovakia*
[3] *Instytut Fizyki Teoretycznej i Astrofizyki, Uniwersytet Gdański, PL-80-952 Gdańsk, Poland*

Bit commitment is a well known cryptographic primitive used as a subroutine for different cryptographic protocols. Unfortunately, it is known to be impossible to implement without additional assumptions, such as limiting the computation power of the adversary. Relativistic bit commitment relays on a more general feature, namely the impossibility of instantaneous communication between distant parties. In this paper we first derive a tight classical upper bound for the winning probability for a specific family of non-local games, known as $\mathrm{CHSH}_q(p)$ and introduced recently in [1]. Using our bound, we discuss possible improvements in security of a security of relativistic bit commitment of Lunghi *et. al.* [2] against classical adversaries. For full version of the paper see [arXiv:1601.08095].

Introduction. Non-local games are important tools of recent quantum information theory. In a two-player non-local game a referee interacts with non-communicating players who cooperate in order to win the game. The referee chooses a pair of questions x, y according to a publicly known probability distribution $r(x, y)$ and sends one question to each player. The goal of the players is to produce outputs a and b. The win or loss of the players is determined by a public verification function $V(a, b, x, y) \in \{0, 1\}$ – if a and b are valid answers for question pair (x, y), the verification function is equal to 1 and the players win the game. With every game G we can associate two different values: the maximum winning probability of classical players $\omega(G)$ and the maximal winning probability of players with quantum resources $\omega^*(G)$. Finding any of these values is generally a hard problem.

Non-local games studied in quantum information science typically satisfy $\omega^*(G) > \omega(G)$. However, many communication scenarios in which non-communicating parties cooperate in order to achieve some goal can be reduced to a non-local game. This is the reason why non-local games are also a valuable tool in various computational complexity scenarios, such as interactive proof systems [3]. A recent result of Chakraborty, Chailloux and Leverrier [1] is a result of this type. They were able to improve the security of a relativistic bit-commitment protocol of Lunghi *et. al.* [2] against classical adversaries into their ability to win a specific family of non-local games called $\mathrm{CHSH}_q(p)$.

$\mathrm{CHSH}_q(p)$ is a family of games generalizing the well known CHSH game [4]. In the CHSH game two non-communicating players receive a single bit input x and y distributed independently and uniformly. Their goal is to provide a single bit answers a and b. They win the game if $a + b = xy \mod 2$.

Recently, there has been some interest in the generalization of this game into higher alphabet inputs and outputs [5]. Family of such games is called CHSH_q. In these games the non-communicating players receive uniformly distributed inputs $x, y \in \mathbb{F}_q$ and produce outputs $a, b \in \mathbb{F}_q$. They win the game if $a + b = xy$, where addition and multiplication are both operations in $\mathbb{F}_q$.

Further generalization of the CHSH_q games into $\mathrm{CHSH}_q(p)$ games concerns the probability distribution of the inputs. $\mathrm{CHSH}_q(p)$ denotes a family of games with CHSH_q verification function, where Bob's input is distributed uniformly, while the distribution of Alice's input is independent of Bob's and is distributed according to some probability distribution, for which $p_{\max} \leq p$, where $p_{\max}$ is the probability of the her most probable input. Note that the games in this family differ only in the probability distribution of Alice's input. In this paper we derive an upper bound on the classical value of these games, which doesn't depend on the concrete distribution, but only on parameters p and q. With a slight abuse of notation, we call this upper bound $\omega(\mathrm{CHSH}_q(p))$ and formally define it as $\omega(\mathrm{CHSH}_q(p)) = \max_i(\omega(G_i))$, where the maximum is taken over all games $G_i \in \mathrm{CHSH}_q(p)$.

Result. Chakraborty, Chailloux and Leverrier [1] give the following upper bound

$$\omega(\mathrm{CHSH}_q(p)) \leq p + \sqrt{\frac{2}{q}}. \tag{1}$$

In our paper [arXiv:1601.08095] we derive a new upper bound for this family of games, which holds whenever $p \geq \frac{1}{\sqrt{2q}}$:

$$\omega(\mathrm{CHSH}_q(p)) \leq p + \frac{1}{2pq}. \tag{2}$$

Our bound is better than the bound (1) in all instances where it holds and in fact, for certain range of parameters q and p it is tight as well. The bound has been found by reducing the problem of finding the best classical strategy for the $\mathrm{CHSH}_q(p)$ games to a problem of finding the maximum amount of incidences between sets of points and sets of lines in finite fields. This technique was introduced by Bavarian and Shor [5] in order to find upper bounds on classical winning probability of CHSH_q games with uniform inputs.

What follows is a brief explanation of how upper bounds on the family of $\mathrm{CHSH}_q(p)$ games can be used to prove security of a relativistic bit-commitment of [2].

Bit-commitment. Each bit-commitment protocol has two phases – the *commit* phase and the *reveal* phase. In the commit phase prover P sends a message to verifier V, in which she commits to a bit x. In the reveal phase, P reveals the bit she committed to in the first phase. There are two security requirements – the *binding* property and the *hiding* property. Bit-commitment protocol is hiding, if V cannot find out value of x before the reveal phase; and it is binding, if P cannot reveal $\overline{x}$ in the reveal phase if she committed to x in the commit phase. It has been shown that both of these requirements cannot be met without additional assumptions.

Here we consider a protocol, where the prover is split into two non-communicating agents P and Q. We enforce the non-communication assumption via relativistic effects – placing P and Q far apart, so they cannot communicate instantly. Obvious downside of such protocol is that binding property can be preserved only for the time it takes a signal from P to reach Q. This limitation can be circumvented by *sustain* phase, in which P and Q continually exchange messages with V in such a way that the protocol remains binding, until the reveal phase. Such protocols were pioneered by Kent [6] and recent state of the art protocol of this type is due to Lunghi *et al.* [2]. The protocol is as follows:

1. Preparation. P and Q share k random numbers $b_1, \ldots, b_k \in \mathbb{F}_q$ and V has k random numbers $y_1, \ldots, y_k \in \mathbb{F}_q$.

2. Commit phase. V sends y_1 to P who replies with $a_1 = b_1 + (y_1 \cdot x)$.

3. Sustain phase. V sends y_2 to Q who replies with $a_2 = b_2 + (y_2 \cdot b_1)$. Sustain phase continues in this fashion with alternate communication between V and P or Q. The timing of messages is crucial part of the sustain phase. If in round i verifier V communicated with $P(Q)$, in round $i+1$ prover $Q(P)$ has to send a_{i+1} before challenge y_i could travel the distance between P and Q.

4. Reveal phase. The prover which did not communicate with V in the last round sends b_k and x to V. V iteratively verifies whether $a_i = b_i + (b_{i-1} \cdot y_i)$ for all $k \geq i \geq 2$ and whether $a_1 = b_1 + y_1 \cdot x$.

It is easy to see that this protocol is hiding, therefore here we discuss only its binding property. Let p_0 and p_1 be the probability that Q reveals 0 and 1 successfully. Protocol is ε-binding, if $p_0 + p_1 \leq 1 + \varepsilon$.

Since this protocol runs in multiple rounds, we are interested in the binding property after k rounds of communication. Let us denote p_0^k and p_1^k the probability to reveal 0 and 1 respectively after k rounds of the protocol. We would like to quantify ε_k, such that $p_0^k + p_1^k \leq 1 + \varepsilon_k$.

The classical value of games in $\mathrm{CHSH}_q(p)$ can be used to show the security of the protocol in the following way.

Throughout the protocol the provers have to provide answers a_i to the challenges y_i. Due to the relativistic constrains message a_i can be seen as a function of the to-be-revealed bit x and challenges $y_i, y_{i-2}, \ldots, y_2, y_1$ (a_i has to be sent before y_{i-1} can reach the active prover). In this view, messages b_i can be recursively defined as $b_i = a_i - (y_i \cdot b_{i-1})$, therefore each b_i can be seen as a function of $y_i, \ldots, y_1, x$.

In the last round the revealing prover (say P) is supposed to reveal b_k. Since P does not know the last challenge y_k yet, he needs to attempt to guess b_k without it. Therefore his strategy can be seen as a function of the previous challenges (which he already knows, since enough time passed since they were sent) and x: $b'_k(y_{k-1}, \ldots, y_1, x)$. The probability to reveal x with given history of challenges $p_x^k(y_{k-1}, \ldots, y_1)$ in this scenario is the probability that $b'_k = b_k$. Since we can treat b'_k as a deterministic function, here the probability is taken only over all possible y_k.

The overall probability to reveal x after k rounds can then be recovered by taking the expectation of $p_x^k(y_{k-1}, \ldots, y_1, x)$ over the history of challenges $y_{k-1}, \ldots, y_1$. However, let us start only by taking expectation over the challenge y_{k-1}, i. e., let us examine $p_x^k(y_{k-2}, \ldots, y_1)$. We are therefore interested in $Pr\left(b'(y_{k-1}, \ldots, y_1, x) = b(y_k, \ldots, y_1, x)\right)$, where the probability is taken over all y_k and y_{k-1}. After rewriting b_k, we get that we are interested in the probability that $b'(y_{k-1}, \ldots, y_1, x) = a_k(y_k, \ldots, y_{k-2}, y_1, x) - y_k \cdot b_{k-1}(y_{k-1}, \ldots, y_1, x)$. Rewriting and leaving out the variables we get $a_k - b'_k = y_k \cdot b_{k-1}$. This can be treated as a non-local game, where Q receives a uniform question $y_k \in \mathbb{F}_q$, P receives a challenge b_{k-1} (which he can reconstruct from challenges known to him at this time) and they are supposed to produce answers b'_k and a_k fulfilling the above condition.

Distribution of y_k is uniform, therefore it remains to examine how well Q can guess the value of b_{k-1} without the knowledge of y_{k-1} – this is in fact $p_x^{k-1}(y_{k-2}, \ldots, y_1, x)$! Therefore this game is in family $\mathrm{CHSH}_q(p_x^{k-1}(y_{k-2}, \ldots, y_1, x))$. Altogether we have $p_x^k(y_{k-2}, \ldots, y_1) \leq \omega(\mathrm{CHSH}_q(p_x^{k-1}(y_{k-2}, \ldots, y_1, x)))$. Better bounds for $\mathrm{CHSH}_q(p)$ games therefore provide better bounds on binding property of this protocol.

[1] K. Chakraborty, A. Chailloux, and A. Leverrier, Phys. Rev. Lett. **115**, 250501 (2015).

[2] T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, S. Wehner, and H. Zbinden, Phys. Rev. Lett. **115**, 030502 (2015).

[3] M. Ben-Or, S. Goldwasser, J. Kilian, and A. Wigderson (ACM, New York, NY, USA, 1988) pp. 113–131.

[4] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).

[5] M. Bavarian and P. W. Shor (ACM, New York, NY, USA, 2015) pp. 123–132.

[6] A. Kent, J. Cryptology **18**, 313 (2005).

Quantum Key Distribution Network for Multiple Applications

A. Tajima[1(a)], T. Kondoh[2(a)], T. Ochi[3(a)], M. Fujiwara[4(b)], K. Yoshino[5(a)], H. Iizuka[6(a)], T. Sakamoto[7(a)], A. Tomita[8(c)], E. Shimamura[9(a)], S. Asami[10(a)], and M. Sasaki[11(b)]
(a) NEC Corporation, 211-8666
(b) National Institute of Information and Communications Technology, 184-8795
(c) Hokkaido University, 060-0808

Abstract. The basic architecture and functions of a quantum key distribution (QKD) network with enhanced application interfaces for applying QKD technologies to multiple applications are proposed. The proposed network has a three-layer architecture that consists of a quantum layer, key management layer, and key supply layer. Since a robust quantum layer is important for constructing a practical QKD network, a QKD system was developed on the basis of a planar lightwave circuit interferometer, and its long-term stable operation was confirmed. A quantum key distribution advanced encryption standard (QKD-AES) hybrid system and an encrypted smartphone system were developed as secure communication applications on our QKD network. The validity and the usefulness of the systems were demonstrated on the Tokyo QKD Network testbed.
Keywords: QKD, QKD Network, AES, BB84

1. Introduction

Communication technology for protecting significant, secret information from eavesdropping and cracking is indispensable. For secret communication, an ultimate, secure form of crypto-key sharing between remote parties is needed. Quantum key distribution (QKD) [1] provides a solution to the problem with a remote user sharing crypto-key. Long-term (over 30-days) field evaluations [2] [3] and QKD network testbeds [4] [5] toward practical use have been reported. We demonstrated a secure TV conference that used point-to-point (PTP) communication and was encrypted by a one-time-pad (OTP) encryption with a quantum-key on the Tokyo QKD Network [5]. In order to build a secure crypto-key distribution network infrastructure that supports not only PTP communications but multipoint-to-multipoint (MPTMP) communications with QKD, novel network architecture, crypto-key management, and key supply functions are needed. In this paper, we first propose the basic architecture and functions of our QKD Platform (PF), which is a QKD network with enhanced application interfaces. We next explain our latest robust QKD system, which serves as a basis for QKD PF and the developed secure communication applications on the QKD PF.

2. Quantum Key Distribution Platform

Secure communication between a data center and a remote backup center is a use case of high-speed secure PTP communication on the QKD PF. Expected applications for the QKD PF include not only PTP systems but also MPTMP systems such as those that enable secure smartphone communication between multiple terminals.

1 a-tajima@bk.jp.nec.com
2 t-kondou@db.jp.nec.com
3 t-ochi@cp.jp.nec.com
4 fujiwara@nict.go.jp
5 yoshino@bp.jp.nec.com
6 h-iizuka@bu.jp.nec.com
7 t-sakamoto@dh.jp.nec.com
8 tomita@ist.hokudai.ac.jp
9 e-shimamura@bp.jp.nec.com
10 shione-asami@bc.jp.nec.com
11 psasaki@nict.go.jp

Therefore, an application independent crypto-key supply that corresponds to MPTMP communication is an important requirement for the QKD PF. Since there are several kinds of QKD protocols, e.g., BB84 and continuous variable protocols, the second requirement is a crypto-key management that corresponds to various types of QKD systems. Also, the QKD PF should support a wide variety of network topologies. In order to meet the above requirements, we propose a three-layer QKD PF architecture that consists of a quantum layer, a key management layer, and a key supply layer as shown in Fig. 1. In the quantum layer, each QKD link generates quantum-keys in its own way. The keys are then pushed up to the key management layer, stored, relayed, and managed, supporting various network topologies and multiple user applications. The key supply layer is introduced to implement two functions: an application independent key supply and a secure key transfer from the QKD PF to key consumers. The QKD PF uses a centralized control style. A key management server monitors the status of the QKD PF such as the error rates of the QKD links and the accumulation of generated keys. The key management server also decides the key relay route. The Tokyo QKD Network was updated and has been operated on the network architecture [6].

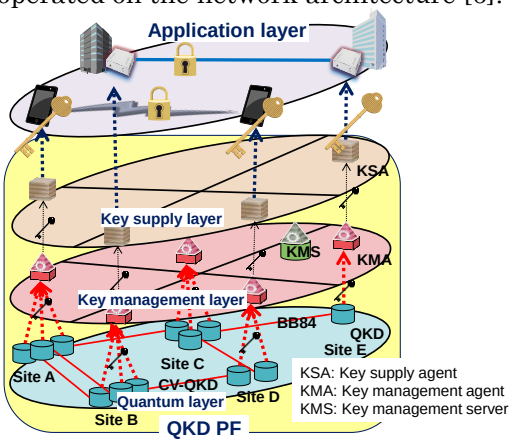


Fig. 1 QKD PF architecture

3. Robust QKD System

For practical operation of the QKD PF, a robust quantum layer is indispensable. We developed a robust, single-way decoy-BB84 [7] QKD system on the basis of a planar lightwave circuit interferometer that operates with a low quantum bit error rate (QBER) [3]. A layer 2 network encryptor was integrated with the QKD system (QKD-AES hybrid system in Sec. 4), and long-term operation under practical environmental conditions was carried out. Consecutive stable operation for 21 weeks was achieved. Fig. 2 shows the evaluation results. An average secure key rate of 107.7 kbps (@11.5 dB loss) with standard deviation of +/-8.6% was confirmed.

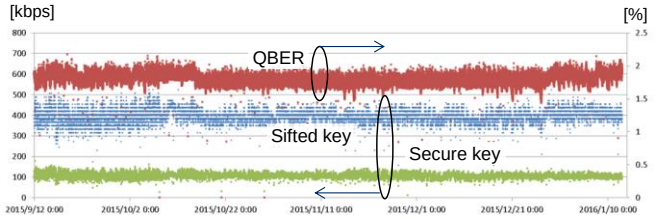


Fig. 2 Long-term evaluation results

4. Applications on the QKD PF

In this section, examples of applications implemented so far on the QKD PF are introduced. One application is a quantum key distribution advanced encryption standard (QKD-AES) hybrid system for high-speed (> Gbps) secure communication. As shown in Fig. 3, a layer 2 network encryptor was integrated with the QKD PF. Synchronization of the crypto-key between terminals is a key technology. In the application, data over Ethernet was encrypted with AES, and the crypto-key was periodically refreshed from the QKD PF. We confirmed a key refresh period of several seconds and long-term (21-week) stable operation.

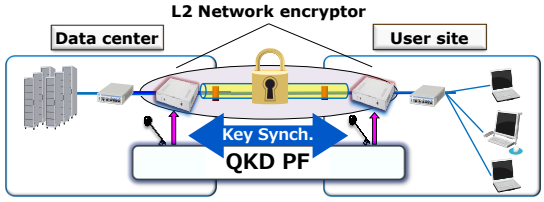


Fig. 3 QKD-AES hybrid system

The second application is an encrypted smartphone system that corresponds to multiple users. Fig. 4 shows an overview of the application. A center server manages both call sessions and crypto-key distributions. To realize MPTMP secure communication, call sessions are encrypted with AES, and quantum keys are used for authentications and AES crypto-key distributions. An AES crypto-key is distributed with OTP from the center server. On the QKD PF with 5 nodes, we confirmed a sequence of key distributions from the QKD PF to smartphones and secure communication between each smartphone.

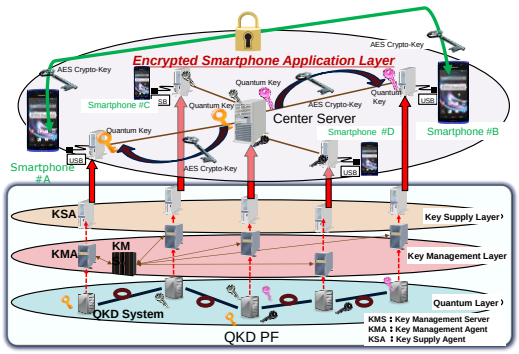


Fig. 4 Encrypted smartphone system

5. Summary

The basic architecture and functions of a QKD network with enhanced application interfaces have been explained for multiple secure communication applications. Robust QKD systems are integral for QKD networks. We have presented the long-term, highly stable operation of our QKD system. As examples of secure communication applications on the QKD PF, a QKD-AES hybrid system and a secure smartphone system have been introduced. With these technologies, we believe that secure communication infrastructure will be constructed in the near future.

Acknowledgements

Part of this work was supported by a NICT-commissioned research program.

References

[1] C. H. Bennett and G. Brassard. Quantum Cryptography: Public key distribution and coin tossing. Proc. Int. Conf. Comput. Syst. Signal Processing, Bangalore, 1984, pp. 175–179, 1984.

[2] A. R. Dixon, J. F. Dynes, M. Lucamarini, B. Fröhlich, A. W. Sharpe, A. Plews, S. Tam, Z. L. Yuan, Y. Tanizawa, H. Sato, S. Kawamura, M. Fujiwara, M. Sasaki, and A. J. Shields. High speed prototype quantum key distribution system and long term field trial. Optics Express Vol. 23, Issue 6, pp. 7583–7592, 2015.

[3] K. Yoshino, T. Ochi, M. Fujiwara, M. Sasaki, and A. Tajima. Maintenance-free operation of WDM quantum key distribution system through a field fiber over 30 days. Optics Express, Vol. 21, Issue 25, pp. 31395–31401, 2013.

[4] M. Peev and the SECOQC collaboration. The SECOQC quantum key distribution network in Vienna. New J. Phys. 11, 075001/1-37, 2009.

[5] M. Sasaki and the Tokyo QKD Network collaboration. Tokyo QKD Network and the evolution to Secure Photonic Network. Proc. OSA/ CLEO 2011, JTuC1, 2011.

[6] Tokyo QKD Network at present. URL: http://www.tokyoqkd.jp/

[7] H. –K. Lo, X. Ma, K. Chen. Decoy state quantum key distribution. Phys. Rev. Lett. 94, 230504, 2005.

New Technologies by Fusion of Macroscopic Quantum Physics and Classical Information Science

Osamu Hirota[1] *

[1]*Quantum ICT Research Institute, Tamagawa University,*
6-1-1,Tamagawa-gakuen,Machida city, Tokyo, Japan

Abstract. Quantum information science is not merely a field of physics but a new science which aims to create new scientific technologies by combining the conventional information science and quantum physics. While information science focuses on the technologies which are useful in the real world, quantum physics aims at understating the characteristics of the physical world. In order to develop the above-captioned new science, we must take full advantage of the characteristics of both information science and quantum physics. To that end, it is inevitable to apply macroscopic quantum physics to classical information science. This talk will deal with the non-orthogonal quantum state in the infinite-dimensional space, a representative example of macroscopic quantum effects, as well as its history. In addition, the basic concepts of" Quantum Enigma Cipher " and " Quantum Radar Camera "are introduced, which have been developed based on the said study. These are expected to be applied in a real world as commercial technologies.

Keywords: Macroscopic quantum phenomena, Quantum Enigma Cipher, Quantum Radar Camera

1 Introduction

Many fundamental theories in quantum information science were developed based on non-orthogonal quantum state in infinite dimensional space, which describes a macroscopic quantum phenomena. A problem of discrimination of non-orthogonal quantum states through quantum measurement, that was pioneered by C.W.Helstrom[1], is a typical example. To formulate quantum communication theory, several researchers generalized from Bayes criterion to Neyman-Peason , Minimax criteria, and Shannon mutual information which play different roles in each other. These provide useful tool for technologies of classical information processed by quantum phenomena. Thus, theory of non-orthogonal state in infinite dimensional space is a foundation for quantum information science which opens up new technologies in a real world.

In this paper, I describe a survey of my works on quantum information science based on a fusion of macroscopic quantum physics and classical information science. First, I describe a survey of theory of non-orthogonal quantum state in the sections II and III, including a basic theory for quantum information science such as quantum communication theory. In the section IV, I discuss an application of theoretical achievements on non-orthogonal quantum state to a new concept on cryptography such as open system cryptography. In the section V, an example of a new physical cipher such as open system cryptography so called Quantum Enigma Cipher is described, in which the security is ensured by a combination of a mathematical encryption and physical randomization of its ciphertext.

Furthermore, it will be suggested for future works that quantum imaging has a potential of a real application for a new type of camera so called quantum radar camera by connecting the original theory and Volterra-Wiener theory.

*hirota@lab.tamagawa.ac.jp

2 Basis of quantum optics

2.1 Quantum optical field

Glauber unified a formulation on classical and quantum optical field that is described by

$$\bigtriangledown^2 E(r,t) = \frac{1}{c^2}\frac{d^2E(r,t)}{dr^2} \tag{1}$$

where the electric field is given by

$$E(r,t) = i\sum_k (\frac{h\omega_k}{4\pi\epsilon_0})^{1/2}[a_k u_k(r)e^{-i\omega_k} - {a_k}^\dagger u_k(r)e^{i\omega_k}] \tag{2}$$

Here $u_k(r)$ is mode function. This mode is called Q-mode which corresponds to infinite dimensional Hilbert space H_S. Observables in the mode are described by photon annihilation and creation operators as follows:

$$\begin{aligned} a &= (X_C + iX_S) \\ a^\dagger &= (X_C + iX_S) \end{aligned} \tag{3}$$

where $[a_k, a^\dagger_{k'}] = \delta_{k,k'}$.

The quantum state is a vector in the space H_S.

$$\begin{aligned} |\Psi> &\in H_S \\ |||\Psi>|| &= 1 \end{aligned} \tag{4}$$

where whole state vectors are normalized.

2.2 Basic states of Q-mode

Since Q-mode means an infinite dimensional Hilbert space, the state vector is represented by a linear superposition of orthonormal vector such as Fock state $|n>$. The representative state is a coherent state which was discussed by R.Glauber[2] to explain coherence property of laser light. Then coherent state is given

$$\begin{aligned} a|\alpha> &= \alpha|\alpha> \\ |\alpha> &= \sum_n \frac{\alpha^n}{n!}e^{-|\alpha|^2/2}|n> \end{aligned} \tag{5}$$

where

$$\begin{aligned} \alpha &= <\alpha|a|\alpha> = < X_c > + i < X_s > \\ |\alpha|^2 &= < n > = <\alpha|a^\dagger a|\alpha> \end{aligned} \quad (6)$$

The coherent state is a typical example of the non-orthogonal state in Q-mode as follows:

$$<\alpha_1|\alpha_2> = exp(-\frac{1}{2}|\alpha_1|^2 - \frac{1}{2}|\alpha_1|^2 + \alpha_1^*\alpha_2) \quad (7)$$

This provides the over completeness in the space such as

$$\frac{1}{\pi}\int |\alpha><\alpha| d^2\alpha = I \quad (8)$$

where I is the identity operator on H_S.

2.3 Glauber-Sudarshan representation

The Galuber-Sudarshan representation is for describing the phase space distribution of a quantum system in the phase space formulation. It provides useful applications in laser theory and especially coherence theory, and given as follows[2,3]:

$$\begin{aligned} \rho_{GS} &= \int P(\alpha)|\alpha><\alpha| d^2\alpha \\ \Xi(\lambda) &= \int <\alpha|e^{\lambda a^\dagger - \lambda^* a}|\alpha> P(\alpha) d^2\alpha \end{aligned} \quad (9)$$

First order mutual coherence function is defined as follows:

$$G^1(r_1, r_2, \tau) = Tr\{\rho_{GS} E^\dagger(r_1, t_1) E(r_2, t_2)\} \quad (10)$$

Higher order mutual coherence function can also be defined. Here we give the second order mutual coherence function.

$$\begin{aligned} & G^2(r_1, r_2, \tau) \\ & = Tr\{\rho_{GS} E^\dagger(r_1, t_1) E^\dagger(r_2, t_2) E(r_2, t_2) E(r_1, t_1)\} \end{aligned} \quad (11)$$

In the subsequent sections, I will provide useful applications of the above theories.

3 Main theorems in quantum information science

A role of quantum information science is to verify potential applications of fundamental nature of quantum mechanics. To do so, quantum communication theory was developed. In this section, I will describe the fact that non-orthogonal states play a very important role in such a theory.

3.1 Quantum detection theory for non-orthogonal states

Quantum detection theory makes clear the fundamental limit for the discrimination among quantum states. Basically, if a set of quantum states is non-orthogonal each other, no one can discriminate without error. In the following, the formulations are shown.

Let us first describe the theory of quantum Bayes criterion.

Theorem:$\{Helstrom\}$[1]
The quantum limitation (average error probability) for the discrimination for two quantum states ρ_1 and ρ_2 is given by

$$P_e = \frac{1}{2} - ||p_1\rho_1 - p_2\rho_2|| \quad (12)$$

where p_1, and p_2 are a priori probabilities.

Let us generalize to M-ary case. That is, a set of quantum states is given as $\{\rho_i, i = 1, 2, 3, \dots M\}$. The criterion of quantum Beys strategy is as follows:

$$\min_{\mathbf{\Pi}} \sum_i \sum_j \xi_i C_{ji} Tr \rho_i \Pi_i \quad (13)$$

where, $\mathbf{\Pi} = \{\Pi_j\}$ is POVM(positive operator valued measure). As usual, we define the risk operator as follows:

$$W_j \equiv \sum_{j=1}^M \xi_i C_{ji} \rho_i \quad (14)$$

$$\Gamma = \sum_{j=1}^M \Pi_j \mathbf{W}_j = \sum_{j=1}^M W_j \Pi_j \quad (15)$$

In general, we consider $C_{ji} = 1\ (i \neq j),\ \ C_{ji} = 0\ (i = j)$. Then the criterion becomes average error probability Pe.

$$\min_{\mathbf{\Pi}} P_e = \min_{\mathbf{\Pi}} (1 - \sum_i \xi_i Tr \rho_i \Pi_i) \quad (16)$$

Theorem:$\{Holevo[4], Yuen[5]\}$
The optimum condition for M-ary quantum Bayes strategy with respect to POVM is

$$\begin{aligned} & (W_j - \Gamma)\Pi_j = \Pi_j(W_j - \Gamma) = 0, \quad \forall j \\ & \Pi_j(W_i - W_j)\Pi_i = 0, \quad \forall i, j \\ & W_j - \Gamma \geq 0, \quad \forall j \end{aligned} \quad (17)$$

where

$$\begin{aligned} W_j &\equiv \sum_{j=1}^M \xi_i C_{ji} \rho_i \\ \Gamma &= \sum_{j=1}^M \Pi_j W_j = \sum_{j=1}^M W_j \Pi_j \end{aligned} \quad (18)$$

where $C_{ji} = 1\ (i \neq j),\ \ C_{ji} = 0\ (i = j)$.

In case of quantum minimax strategy, the criterion is given by

$$P_{em} = \min_{\{\Pi_j\}} \cdot \max_{\{\xi_i\}} \left\{ 1 - \sum_{i=1}^M \xi_i Tr \rho_i \Pi_j \right\} \quad (19)$$

In this criterion, we have the following result.

Theorem:{$Hirota - Ikehara$[6]}
Let $\{\xi_i\}$ and $\{\Pi_j\}$ be a priori probability and POVM, respectively. Then we have

$$\min_{\{\Pi_j\}} \cdot \max_{\{\xi_i\}} P_e = \max_{\{\xi_i\}} \cdot \min_{\{\Pi_j\}} P_e \tag{20}$$

Theorem:{$Hirota - Ikehara$[6]}
The optimum conditions for POVM is given by

$$\begin{aligned} & Tr\rho_i\Pi_i = Tr\rho_j\Pi_j, \qquad \forall i,j \\ & (W_j - \Gamma)\Pi_j = \Pi_j(W_j - \Gamma) = 0, \qquad \forall j \\ & \Pi_j(W_i - W_j)\Pi_i = 0, \qquad \forall i,j \\ & W_j - \Gamma \geq 0, \qquad \forall j \end{aligned} \tag{21}$$

where $C_{ji} = 1 \ (i \neq j), \ C_{ji} = 0 \ (i = j)$.

Recently, the mathematical progress for quantum minimax theory has been given by G.M.D'Ariano et al[7], K.Kato [8], F.Tanaka [9], and K.Nakahira et al [10].

3.2 Classical capacity for quantum Gaussian channel

When Shannon mutual information is employed as a criterion for evaluation of communication performance, collective quantum measurement effect provides the following capacity formula for lossy Gaussian noise channel, which can be realized by coherent state signals or two-photon coherent state. This is quantum version of well known Shannon-Wiener formula in classical Gaussian channel. In fact, when $S \ll < n >$, it reduces to classical one. In addition, several features on difference between quantum and classical of classical capacity for several quantum channels were clarified by author's group.

Theorem:{$Holevo - Sohma - Hirota$[11]}
The classical capacity for quantum lossy Gaussian noise channel is given by

$$\begin{aligned} C_{HSH} &= \log(1 + \frac{S}{1 + < n >}) + S\log(1 + \frac{1}{S + < n >}) \\ &- < n > \log(\frac{1 + \frac{S}{< n >}}{1 + \frac{S}{1 + < n >}}) \end{aligned} \tag{22}$$

where S and $< n >$ are received signal and noise photon number, respectively.

Theorem:{$Hirota$[12], $Guha$[13]}
The secret capacity for physical cipher based on coherent state is

$$\begin{aligned} & C_{GS} = C_{HSH} - C_{Shannon} = \log(1 + \frac{S^B}{1 + < n >^B}) + \\ & S^B \log(1 + \frac{1}{S^B + < n >^B}) - < n >^B \log(\frac{1 + \frac{S^B}{< n >^B}}{1 + \frac{S^B}{1 + < n >^B}}) \\ & - \log(1 + \frac{S^E}{1 + < n >^E}) \end{aligned} \tag{23}$$

3.3 No-cloning theorem

Theorem:{$Wootters - Zurek$[14]}
Let us assume that $|\psi >_A, |\phi >_B$ are quantum states in two systems. There is no unitary operator on $H \otimes H$ such that for all states $|\psi >_A$,$|\phi >_B$

$$U(|\psi >_A \otimes |\phi >_B) = e^{ic(\psi,\phi)}|\psi >_A \otimes |\psi >_B \tag{24}$$

where $ic(\psi, \phi)$ is a real number depending on $|\psi >_A$,$|\phi >_B$.

4 Closed system cryptography and open system cryptography

Let us consider a system of symmetric key cipher such as stream cipher where $|K_s|$ bits secret key K_s is shared between the sender and the receiver, and $|K_s|$ bits secret key is expanded by a mathematical algorithm, which is called running key. The ciphertext is given by " exclusive OR operation " of running key sequence and plaintext sequence. In this system, the sequence of ciphertext is determined uniquely by the sequences of running key and plaintext. Although the running key is longer than $|K_s|$ bits, the possible number of sequence is only

$$N = 2^{|K_s|}, \tag{25}$$

because mathematical algorithm as expander is deterministic for $|K_s|$ bits secret key as an initial key.

The ciphertext is sent to the legitimate receiver through a transmission line. The attacker can get the exact ciphertext by tapping on the line. That is, the ciphertext of the attacker is the same as that of legitimate receiver. This scheme is called " closed system cryptography ". In general, the attacker can pin down the $|K_s|$ bit secret key by a brute force attack under certain known plaintext, because the key space is formed only by $|K_s|$ bits in closed system cryptography. On the other hand, one can employ random algorithm as expander. However, because of the conditions that the legitimate receiver has to decrypt ciphertext by $|K_s|$ bits key and that ciphertexts for the legitimate receiver and the attacker are same, such a randomization cannot provide an expansion of key space. Such a feature is unavoidable in the closed system cryptography.

In order to investigate a new cryptosystem, we have to find " open system cryptography " to realize the scheme where the key space for the attacker is greater than that for the legitimate receiver. By open system cryptography, we mean a cryptosystem such that ciphertext of the legitimate receiver and ciphertext of the attacker are different. In this system, the attacker does not receive the ciphertext correctly, and cannot pin down the $|K_s|$ bit secret key even if she tries a brute force attack. However, the legitimate receiver can obtain the long plaintext sequence correctly from the received signal based on $|K_s|$ bit key. Since it seems impossible to realize such a scheme only by mathematical tool, one needs a help of physical phenomena to attain the goal. In the following section, I will explain a potential method to realize the above scheme.

5 Quantum Enigma Cipher

In this section, I will give a general framework of a physical cipher as application of quantum detection theory and no cloning theorem for non-orthogonal states.

5.1 Concept

The general network systems need to be protected from interception by unauthorized parties. The most serious attack is " Cyber attack against Layer-1 (physical layer such as optical communication line)", because technologies of coupler for tapping have been developed by several institutes. In addition, there are many optical monitor ports for network maintenance. In fact, physical layer of high speed data link is a defenseless. To date, that protection has been provided by classical encryption systems. However, such technologies cannot ensure the provable security, and also the eavesdropper can obtain the correct ciphertext: C of mathematical cipher for payload at Layer-2, and she can store it in memory devices. Thus, we cannot rule out the possibility that the cipher may be decrypted by future development of algorithm and computer science.

The best way to protect high speed data is to physically randomize signals as the ciphertext of a mathematical cipher. This is called physical random cipher. The most important feature of this physical random cipher is that the eavesdropper cannot get the correct ciphertext of mathematical cipher, for example a stream cipher by PRNG (pseudo random number generator), from communication lines, while the legitimate user can get it and he can decrypt based on a knowledge of secret key of PRNG.

First example was proposed by H.P.Yuen as "Keyed communication in quantum noise(KCQ)"in 2000[review is given in 15]. In his scheme, the mathematical cipher is used to select optical communication basis to transmit binary bit data. So the optical signals correspond to ciphertext of the mathematical cipher. Thus a modulation scheme becomes an encryption box for electric data sequence. A legitimate user can get the correct ciphertext, but an eavesdropper cannot get the correct ciphertext, because she does not know which communication basis is used and her received signals are randomized by large effect of quantum noise due to mismatch in communication basis.

During 15 years, many prototype systems so called α/η or Y-00 protocol have been implemented and useful performances have been demonstrated in real optical networks[16,17,18,19].

5.2 Definition of Quantum Enigma Cipher

Quantum Enigma Cipher is a general scheme for physical random cipher, which may be a generalization of KCQ. Let us describe here the ideal quantum enigma cipher system.

The quantum enigma cipher consists of an integration of mathematical encryption box and physical randomization box. Here, the physical randomization means that optical signals as the ciphertext of a mathematical cipher are randomized by quantum noise when the eavesdropper observes optical signals with coherent states or another non-orthogonal state. Along with this concept, Quantum Enigma Cipher allows a secure high speed data transmission by means of the quantum noise randomization by a mathematical encryption box and signal modulation systems. Thus, we will define the quantum enigma cipher.

Definition Quantum Enigma Cipher is defined as a scheme which has the following property[20,21,22,23]: Optical signals correspond to ciphertext of a mathematical cipher. The observation signals of legitimate's receiver are error free with a priori knowledge in communication systems. An eavesdropper's receiver suffer a serious error without a priori knowledge.

Examples of the implementation are as follows:
(a) Communication basis for transmission of data is scrambled by PRNG with a secret key[15].
(b) Mapping scheme between data for communication system and optical signal is scrambled by PRNG [24].
(c) Fusion of (a) and (b)[24]
(d) A priori probability for a set of coherent states is hidden as secret key against eavesdropper[21].
(e) A difference of error performance between legitimate and eavesdropper's receiver is created by entanglement resource in transmitter and receiver[22,25].

If the data for communication system is not encrypted by a mathematical cipher, one has to employ (a),(b) and (c). If the data is already encrypted by a mathematical cipher, one can employ one of $\{(d),(e)\}$.

In any scheme, the quantum enigma cipher has a mathematical encryption box and physical encryption box. The mathematical encryption box has a secret key of the length $|K_s|$ bits and PRNG for expansion of the secret key. The physical encryption box has a mechanism to create ciphertext as signal and it has a function to induces an error when the eavesdropper's receiver receives the ciphertext as signal. Consequently different ciphertext sequences are observed in the legitimate's receiver and the eavesdropper's receiver, respectively. A requirement for the physical randomization is

$$P_e(Eve) >> P_e(Bob) \sim 0 \tag{26}$$

This means that the error performance P_e of the eavesdropper becomes worse than that of the legitimate user, when they observe the ciphertext as signal in communication lines.

5.3 Security analysis

In the investigation for the quantitative evaluation of information theoretically secure scheme, Shannon mutual information, trace distance (statistical distance), and Holevo quantity are not appropriate as measure of security. In the following, we will give a guide for such a purpose.

5.3.1 Model

Let us describe a standard symmetric key encryption. A general symmetric key encryption Λ can be given by

$$\Lambda = ([P_K], Enc, Dec) \tag{27}$$

where $[P_K]$ is key generation algorithm and it provides key sequence $K \in \mathcal{K}$ depending on the probability P_K, Enc is an encryption algorithm which generates ciphertext $C = Enc(K, M)$ where M is plaintext, Dec is a decryption algorithm which produces plaintext $M = Dec(K, C)$. In the case of symmetric key cipher, the secret key is fixed.

When Λ cannot be decrypted by means of computational resource, its security is evaluated by "Guessing probability"[21,22,23].

(i) Ciphertext only attack on data:

$$P_G(M) = \max_{M \in \mathcal{M}} P(M|C) \tag{28}$$

(ii) Ciphertext only attack on key:

$$P_G(K) = \max_{K \in \mathcal{K}} P(K|C) \tag{29}$$

On the other hand, when some plaintext M_k and ciphertext corresponding to them are known, it is called known plaintext attack. It is easy to generalize the above formula as follows:

(iii) Known plaintext attack on data:

$$P_{G_k}(M) = \max_{M \in \mathcal{M}} P(M|C, M_k) \tag{30}$$

(iv) Known plaintext attack on key:

$$P_{G_k}(K) = \max_{K \in \mathcal{K}} P(K|C, M_k) \tag{31}$$

If one needs an average, then one can define average guessing probability as follows:

$$\bar{P_G}(M) = \sum_{C \in \mathcal{C}} P(C) \max_{M \in \mathcal{M}} P(M|C) \tag{32}$$

In order to apply the above concept to quantum enigma cipher, one can employ the quantum detection theory for observation of ciphertext, and easily modify the formula of guessing probability. These are sometimes called maximum "a posteriori probability" guessing.

5.3.2 Evaluation of security

A mathematical encryption box produces the ciphertext of length at most $2^{|K_s|}$ bits. Because the key length is $|K_s|$ bits, when the eavesdropper gets the known plaintext of the length $|K_s|$ bits and ciphertext corresponding to them, she can pindown the secret key by the Brute force attack (trying $2^{|K_s|}$ key candidates). That is, the guessing probability is one. In addition, the sequence of the ciphertext has certain correlation because of the structure of PRNG. So the eavesdropper can investigate several mathematical algorithms to estimate the secret key.

In the ideal quantum enigma cipher, the eavesdropper's observation of the cipertext as signal in communication lines suffers error completely by quantum noise randomization, while the legitimate user does not. So the legitimate user can decrypt with the secret key, but the eavesdropper does not even if she gets the secret key after her observation of ciphertext as signal.

Thus, the guessing probability is

$$P_G(K_s) = 2^{-|K_s|} \tag{33}$$

even if she collects the ciphertext of $2^{|K_s|}$ bits. This means an immunity against the Brute force attack by computers. On the other hand, the quantum no cloning theorem may protect a physical Brute force attack by cloning whole quantum states, because a set of quantum states for the quantum enigma cipher are designed by non-orthogonal state with very close signal distance each other.

Recently, 1 Gbit/sec physical random cipher as a first generation of quantum enigma cipher was demonstrated and Y-00 cipher of 100 Gbit/sec by wave length division multiplex was also demonstrated[19].

6 Security of one time pad

6.1 Ideal

When the distribution P_K is uniform, the one time pad has the perfect secrecy such that

$$P_G(M) = \max_{M \in \mathcal{M}} P(M|C) = P(M) \tag{34}$$

However, even if the system has the perfect secrecy, it does not mean "secure" against known plaintext attack on data when data is a language such as English. That is,

⌈The perfect secrecy means secure against ciphertext only attack, and it does not imply the security against "known plaintext attack and falsification attack".[26]⌋

Thus, the term of "unconditional security" is misleading. Let us show an example. The eavesdropper can get the correct chiphertext of the length $|K|$ bits, and she can launch the Brute force attack. The decrypted data sequences of the length $|K|$ bits give all combination of English alphabet (ASCII code) of length $|K|$ bits. These include a large number of correct English words such as "orange, signal, cipher, and so on". When the attack is ciphertext only attack, she cannot decide which word is the real plaintext. However, if she knows the first alphabet "o" as the known plaintext attack, the correct word may be "orange". Thus, the guessing probability may become very large value.

6.2 Security of one time pad forwarded by QKD

The quantum key distribution does not provide the perfectly uniform distribution for key sequence K_G

against an eavesdropper. In fact, the average guessing probability is given by Portman and Renner[27] as follows:

$$\bar{P}_G(K_G) \leq \frac{1}{2^{|K_G|}} + d \tag{35}$$

where d is the trace distance in QKD protocol. Thus, the one time pad forwarded by QKD is non ideal one time pad which is encrypted by key sequence with non uniform distribution. That is,

$$\Lambda = ([P_K] \neq ideal, Enc, Dec), P_K \neq \frac{1}{2^{|K_G|}} \tag{36}$$

If the value of the trace distance is very large in comparison with $\frac{1}{2^{|K_G|}}$, the guessing probability is very large. So such a one time pad may be decrypted easily.

In addition, QKD needs an initial secret key for the authentification before the legitimate users start the QKD protocol. This is the same situation as the conventional symmetric cipher in which the key is for initial seed key for PRNG. Thus, we cannot start cryptographic action without certain initial secret key, except for the conventional public key encryption.

7 Quantum radar camera

Quantum imaging is one of attractive applications of new physical phenomena. Especially ghost imaging is a technology to synthesize target image by means of certain correlation between signal beam and reference beam. In original proposal[28] and experiment[29], an entanglement light was employed in the system. By lively investigation, it was clarified that ghost imaging does not represent a true quantum, and that the function can be realized by semi-quantum or classical resource. This fact is reasonable in the world of science and technology, because any useful technologies in real world should be realized by classical way, and these functions may be enhanced by quantum nature. The important fact is that this function can be realized only at optical field. In addition, a special feature of ghost imaging is to have immunity against atmospheric turbulence. To analyze it, one can employ the extended Huygens-Fresnel principle.

$$E(r',t) = \int E(r,t) \frac{k_0 e^{ik_0(L+|r'-r|^2/2L)}}{i2\pi L} e^{\phi(r',r)} dr \tag{37}$$

where $\phi(r', r)$ is a complex valued random process due to turbulence.

Thus, based on Glauber's coherence theory and the above formula, unified theory has been presented by Erkmen and Shapiro[30], Hardy and Shapiro[31]. The basic formula is given by following the average cross correlation function.

$$< R(r_{ccd}) >= K \int d\tau_1 \int d\tau_2 \int dr h(t-\tau_1) h(t-\tau_2)$$
$$\times < E_R^{\dagger}(r_{ccd}, \tau_1) E_T^{\dagger}(r, \tau_2) E_R(r_{ccd}, \tau_1) E_T(r, \tau_2) > \tag{38}$$

Their works give a great contribution towards a real development of this technology. However, one can see easily the fact that their model includes highly non-linear random process in which Volterra-Wiener theory is applicable. Based on the above, a general design theory as space-time quantum Wiener receiver theory has been developed by the present author. It has a potential to generalize the ghost imaging as a "quantum radar camera", which is applicable to automobile camera under any weather. I will report in the subsequent paper.

References

[1] Helstrom C.W(1976), Quantum detection and estimation theory, (Academic press, New York).

[2] Glauber R(1963), Coherent and incoherent states of the radiation field, Physical Review, **131**, 2766.

[3] Sudarshan E.E.G(1963), Equivalence of semiclassical and quantum mechanical description of statistical light beam, Physical Review Letters, **10**, 277.

[4] Holevo A.S(1973), Statistical decision theory for quantum systems, Journal of Multivariate Analysis, **3**, 337.

[5] Yuen H.P, Kennedy R and Lax M(1975), Optimum testing of multiple hypotheses in quantum detection theory, IEEE Trans.Information Theory, **21**, 125.

[6] Hirota O, and Ikehara S(1982), Minimax strategy in the quantum detection theory and its application to optical communication,, Trans of the IECE of Japan, **E65**, 627.

[7] D'Ariano G.M, Suchi M.F,and Kahn J(2005), Minimax quantum state discrimination, Physical Review, **A-72**, 032310.

[8] Kato K(2011), Minimax receiver for a binary pure quantum state signal, Proc. of IEEE ISIT at 2011, pp1077-1081.

[9] Tanaka F(2012), Non-informative priori in the quantum statistical model of pure states, Physical Review, **A-85**, 062305.

[10] Nakahira K, Kato K, Usuda T(2013), Minimax strategy in quantum signal detection with inconclusive results, Physical Review **A-88**, 032314.

[11] Holevo.A.S, Sohma.M, and Hirota.O(1999), Capacity of quantum Gaussian channels, Phys. Rev.**A-59**, 1820.

[12] Hirota O, Iwakoshi T,Sohma M, and Futami F(2010), Quantum stream cipher beyond the Shannon limit of symmetric cipher and the possibility of experimental demonstration, Proceedings of SPIE on Quantum communication and quantum imaging, **7815**.

[13] Guha S, Hayden P,Krovi H,Lloyd S,Lupo C,Shapiro J.H, Takeoka M,and Wilde M(2014), Quantum enigma machines and the locking capacity of a quantum channel, Physical Review **X-4**, 011016.

[14] Wootters W and Zurek W(1982), A single quantum cannot be cloned, Nature, **299**, 802.

[15] Yuen H.P (2003), KCQ:A new approach to quantum cryptography I, arXiv.org,quant-ph,arXiv:0311061.

[16] Borbosa G.A, Corndorf E, Kanter G.S, Kumar P, and Yuen H.P(2003), Secure communication using mesoscopic coherent state, Physical Review Letters, **90**, 227901.

[17] Corndorf E, Liang C, Kanter G.S, Kumar P, and Yuen H.P(2005), Quantum noise randomized data encryption for wavelength division multiplexed fiber optic network, Physical Review **A-71**,062326.

[18] Hirota O, Sohma M, Fuse M, and Kato K(2005), Quantum stream cipher by Yuen 2000 protocol: Design and experiment by intensity modulation scheme, Physical Review,**A-72**, 022335.

[19] Futami F(2014), Experimental demonstrations of Y-00 cipher for high capacity and secure fiber communications, Quantum Information Processing, **13**, 2277.

[20] Hirota O (2013), Quantum Enigma Cipher: protecting optical network for cloud computing system, *Reader's Review, United Airline*,vol-70, March 2013.
Hirota O, Cyber attack against optical communication system and its defense technology - Toward development of Quantum Enigma Cipher- , *IEICE Technical Meeting on Optical Commun.System:OCS*, vol-113, no-90, OCS2013-18, June, 2013.
Hirota O and Futami F, Quantum Enigma Cipher, *Manyousya Publishing Company*, in Japanese, Oct. 2013.

[21] Hirota O (2015), Towards quantum enigma cipher-a protocol for Gbit/sec encryption based on discrimination property of non-orthogonal quantum state-, Tamagawa University Quantum ICT Research Institute Bulletin, **5**, 5.

[22] Hirota O (2015), Towards Quantum Enigma Cipher-II, Tamagawa University Quantum ICT Research Institute Bulletin, **5**,33.

[23] Hirota O (2015), Towards Quantum Enigma Cipher-III, Tamagawa University Quantum ICT Research Institute Bulletin, **5**,37.

[24] Hirota O, and Kurosawa K(2007), Immunity against correlation attack on quantum stream cipher by Yuen 2000 protocol, Quantum Information Processing, **vol-6**,81.

[25] Shapiro J.H, Zhang Z,and Wong F.N.C(2014), Secure communication via quantum illumination, Quantum Information Processing, **13**,2171.

[26] Stinson Douglas (1995), Cryptography:Theory and Practice, CRC Press, Inc.

[27] C.Portman and R.Renner(2014), Cryptographic security of quantum key distribution, *arxiv.org:quant-ph*, 1409.3525.

[28] Belinskii A, and Klyshko D (1994), Two photon optics:diffraction, holography,and transformation of two dimensional signals, Soviet Physica JETP, **78**, 259.

[29] Pittman T, Shih Y.H, Strekalov D.V, Sergienko A.V (1995), Optical imaging by means of two photon quantum entanglement, Physical Review, **A-52**, R3429.

[30] Erkmen B.I, and Shapiro J.H (2008), Unified theory of ghost imaging with Gaussian state light, Physical Review, **A-77**, 043809.

[31] Hardy N.D, and Shapiro J.H (2011), Reflective ghost imaging through turbulence, Physical Review, **A-84**, 063824.

Quantum Calderbank-Shor-Steane Stabilizer State Preparation by Classical Error-Correcting Codes

Ching-Yi Lai[1] * Yicong Zheng[2 3] † Todd A. Brun[4] ‡

[1] *Institute of Information Science, Academia Sinica, Taipei, Taiwan 11529*
[2] *Centre for Quantum Technology, National University of Singapore, Singapore 117543*
[3] *Yale-NUS College, Singapore 138614*
[4] *Electrical Engineering Department, University of Southern California, Los Angeles, California, USA 90089*

Abstract. Calderbank-Shor-Steane (CSS) stabilizer states are of particularly importance in the application of fault-tolerant quantum computation (FTQC). However, how to efficiently prepare arbitrary CSS stabilizer states for general CSS stabilizer codes is still unknown. In this paper, we propose two protocols to distill CSS stabilizer states with Steane syndrome extraction by classical codes or quantum CSS codes. With the ability to produce high-quality ancillary states, FTQC schemes using Steane syndrome extraction or those based on teleportation become promising. These ancillary states are expensive and valuable. Along the same lines, we show that classical coding techniques can reduce ancilla consumption by using additional transversal controlled-NOT gates and classical computing power.

Keywords: CSS stabilizer states, Steane syndrome extraction, ancilla distillation, error-correcting codes

1 Introduction

Fault-tolerant quantum computation (FTQC) computes in the codespace of a stabilizer code [1] using imperfect quantum circuits, interspersed with repeated error corrections. Currently most FTQC schemes use Calderbank-Shor-Steane (CSS) type stabilizer codes [2, 3]. We focus on the preparation of the CSS stabilizer states in this talk. Technical details of this work can be found in [4].

CSS stabilizer states can be prepared using Clifford encoding circuits, but this is not fault-tolerant, so the generated states need to be verified. Basic CSS stabilizer states, such as the logical states $|0\rangle_L$ or $|+\rangle_L$, are usually fault-tolerantly generated by specific quantum circuits with post-selection in FTQC schemes. For general CSS codes, it is unknown how to produce arbitrary stabilizer states that are *clean* enough for FTQC, especially when the code length is large. Herein we show how *classical error-correcting codes*, together with *Steane syndrome extraction* [5], can be applied to distill any CSS stabilizer states (Protocol I), by actively correcting errors on a fraction of ancillas. Along the way, we also develop a distillation protocol by using CSS codes rather than classical codes (Protocol II).

2 Ancilla Distillation

Steane suggested a method to extract error syndromes for CSS codes [5], as shown in Fig. 1. Two clean ancillas $|+\rangle_L$ and $|0\rangle_L$ in the logical states of the underlying CSS code $\mathcal{Q}$ are used to measure the X and Z error syndromes, respectively. Each controlled-NOT (CNOT) gate in Fig. 1 represents transversal CNOT gates, and X and Z errors will propagate, respectively, to the ancillas $|+\rangle_L$ and $|0\rangle_L$ through the CNOTs. Suppose the

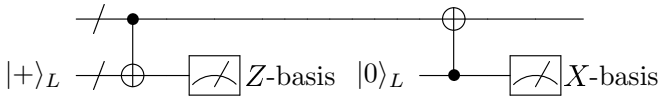


Figure 1: Quantum circuit for Steane syndrome extraction.

measurement outcomes of $|+\rangle_L$ and $|0\rangle_L$ are m_X and m_Z (in bits), respectively. Then the measured X and Z syndromes are $\mathsf{H}_1 m_X^T$, and $\mathsf{H}_1 m_Z^T$, respectively. We can perform error correction according to these syndromes or just keep track of them.

Suppose we are given a bunch of imperfect ancillas in some CSS stabilizer state, and we are going to distill them. It is not efficient to use Steane syndrome extraction to do error correction on a noisy ancilla since it requires us to already have two clean ancillas. What we are going to do is to figure out the correct error syndromes of a small portion of the ancillas by measuring the rest. Our distillation protocol for CSS stabilizer states by classical codes (Protocol I) involves two rounds of error corrections: one for X errors and one for Z errors. Suppose $\mathcal{C}_2$ is an $[m, k, d]$ binary linear block code that can correct $t = \lfloor \frac{d-1}{2} \rfloor$ errors. Such a code has $r = m - k$ parity checks and let $\mathsf{H}_2 = [\mathsf{A}^T \ \mathsf{I}_r]$ be the parity-check matrix of $\mathcal{C}_2$ in the systematic form. In each round, we group the ancillas and do transversal CNOTs on the ancillas according to the pattern of the parity-check matrix H_2. Equivalently the syndromes of target ancillas are encoded by the classical codes into the rest ancillas. Then we can use classical decoding techniques to recover the correct error syndromes on the target ancillas. After two rounds, we are left with a fraction $(\frac{k}{m})^2$ of our original ancillas. The rate of an arbitrary Pauli error is roughly $\tilde{c}p^{t+1}$ for some $\tilde{c}$ if we assume the distillation circuits are perfect. This procedure could be iterated; or one can just vary

*cylai0616@iis.sinica.edu.tw
†zheng.yicong@quantumlah.org
‡tbrun@usc.edu

the distances of the classical codes used depending on the original error rates and the desired final error rates. Similarly for Protocol II by quantum CSS codes.

Our distillation protocols are similar to magic state distillation, but there is an important distinction: because these ancillas are stabilizer states, they can be made using only Clifford gates. We should expect better performance here than in magic state distillation, where one cannot improve the quality of the encoded state directly by measuring it. At the very least we should be able to do better in this respect: with magic state distillation, there is a probability of failure, where you have to discard everything; here, if we detect an error in the logical operators, we can correct them. Also, only certain codes with special properties can be used for magic state distillation; while a broad range of classical error-correcting codes can be applied in our scheme.

3 Ancilla Saving

Steane syndrome extraction is more suitable for quantum CSS codes, whose stabilizer generators have high weight, regardless of locality of the stabilizers. However, it requires two ancillas of the same size of the underlying quantum codes, which makes Steane syndrome extraction expensive especially when code length is large. As a consequence, we would like to save them during syndrome measurement as long as accumulated errors are not serious. It turns out that the ancilla-saving problem is equivalent to the distillation problem mathematically. Parallelling the development of distillation by classical codes, we propose an *ancilla saving* protocol by classical codes.

When the ancilla consumption rate is fixed, we can increase the frequency of quantum error correction with ancilla saving protocol, which equivalently lower the error rate on data qubits. Consequently the effective error rate of the $[[n,1]]+[m,m-r]$ ancilla saving protocol decreases to rp/m, assuming that quantum error correction is sufficiently fast. Let F_{o}^{p} and F_{comb}^{p} be the channel fidelities of the original and the $[[n,1]]+[m,m-r]$ protocols at error rate p, respectively. Then there exists p^* so that $F_{\mathrm{o}}^{p^*}=F_{\mathrm{comb}}^{rp^*/m}$. Hence for $p\leq p^*$ the effective channel fidelity of the $[[n,1]]+[m,m-r]$ protocol is higher. Thus it is possible to use fewer ancillas than necessary to recover correct error syndromes in Steane syndrome extraction by using higher classical decoding complexity and additional CNOTs, while sacrificing a little channel fidelity. It is assumed that classical computing power is much cheaper, compared to expensive quantum resources. The layout of additional transversal CNOTs depends on the chosen classical code and their cost may be comparable to saved ancilla preparation. However, the overall error-correcting power can be increased when the ancilla consumption rate is fixed.

4 Discussion

In the distillation protocol by classical coding, error syndromes of the target ancillas are encoded by the coupling CNOTs and then recovered. If the error rates become small enough, it is no longer reasonable to ignore errors in the transversal circuits, and the measured parity-check syndromes $\mathsf{H}_1\nu_i$ are not reliable. However, this still can be handled by learning more parities of stabilizer generators as suggested in [6]. That is, we choose another classical code $\mathcal{C}_3$ to encode the parity checks of H_1 by appending more redundant rows. By calculating additional parities checks, we can use any decoder of $\mathcal{C}_3$ to purify the decoding outputs of $\mathcal{C}_2$ and obtain more reliable error syndromes about the target ancillas. Technical details and performance analysis are our ongoing work.

With the ability to distill clean logical ancillas, logical teleportation becomes possible [7], since only Clifford gates and logical ancillas are required. One can have an FTQC scheme that consists of several quantum codes suitable for (transversal) implementation of different logical gates and apply logical teleportation to transfer logical qubits between these code blocks [7]. This avoids the need of any magic states. However, the overhead for distillation dominates in this scheme and we need to further analyze and quantify the cost of distillation of various ancillas.

References

[1] D. Gottesman, "Theory of fault-tolerant quantum computation," *Phys. Rev. A*, vol. 57, pp. 127–137, Jan 1998.

[2] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A*, vol. 54, no. 2, pp. 1098–1105, 1996.

[3] A. M. Steane, "Error correcting codes in quantum theory," *Phys. Rev. Lett.*, vol. 77, no. 5, pp. 793–797, 1996.

[4] C.-Y. Lai, Y. Zheng, and T. A. Brun, "Quantum Calderbank-Shor-Steane stabilizer state preparation by classical error-correcting codes," 2016, arXiv:1605.05647.

[5] A. M. Steane, "Active stabilization quantum computation, and quantum state synthesis," *Phys. Rev. Lett.*, vol. 78, no. 11, pp. 2252–2255, 1997.

[6] A. Ashikhmin, C.-Y. Lai, and T. A. Brun. Robust quantum error syndrome extraction by classical coding. In *Proc. IEEE Int. Symp. Inf. Theory*, pp. 546–550, 2014.

[7] T. A. Brun, Y.-C. Zheng, K.-C. Hsu, J. Job, and C.-Y. Lai, Teleportation-based fault-tolerant quantum computation in multi-qubit large block codes. quant-ph/arXiv:1504.03913, 2015.

New quantum error-correcting codes for a bosonic mode

Marios H. Michael[1 2] Matti Silveri[1 3] R. T. Brierley[1] Victor V. Albert[1 *]
Juha Salmilehto[1] Liang Jiang[1] S. M. Girvin[1]

[1] *Departments of Applied Physics & Physics, Yale University, USA*
[2] *Cavendish Laboratory, University of Cambridge, UK*
[3] *Theoretical Physics, University of Oulu, Finland*

Keywords: quantum error-correcting codes, continuous variable, bosonic mode

1 Motivation and intoduction

Successful transmission of quantum information over long distances is a cornerstone of quantum cryptographic protocols and remains a daunting experimental challenge. Photons remain the medium of choice for facilitating such transmissions, and the community has typically focused on transmitting information in only a small number of "flying" photons. Common examples include encoding a qubit in two orthogonal polarizations of a single photon or encoding two qubits in a pair of photons entangled in energy and time [1]. If any such photons are lost during flight, the corresponding encoded information is unrecoverable. However, the large (i.e., infinite) Hilbert space of a photonic mode offers the possibility of utilizing encodings which allow for recovery of the information despite photon loss (or other errors) occurring mid-flight. Needless to say, such encodings are also useful for protecting quantum information in stationary photonic media (e.g., microwave cavities or collective spin systems [2]).

Two classes of single-mode codes have previously been proposed to achieve recoverability: the seminal Gottesman-Kitaev-Preskill (GKP) codes [4, 5], constructed to protect from small shifts in photonic quadratures, and cat-codes [6, 7], consisting of superpositions of evenly distributed coherent states. Code states of both classes consist of superpositions of an infinite number of Fock states, making encoding arguably more complex as compared to code states defined on a finite subspace.

Here, we propose a new class of bosonic codes, *the binomial codes* [8]. The binomial code states are formed from a finite superposition of Fock states weighted with square roots of binomial coefficients. The codes can exactly correct errors that are polynomial up to a specified degree in photonic creation and annihilation operators, including amplitude damping and displacement noise as well as photon addition and dephasing errors. Besides being conceptually simple and highly customizable, binomial codes can protect quantum information from certain errors using a smaller average photon number than the corresponding cat codes. The binomial codes are tailored for detecting photon loss and gain errors by means of measurements of the generalized photon number parity, which is favorable for implementation in state-of-the-art experimental schemes [9]. In Ref. [8], we present an explicit quantum error recovery operation based on projective measurements and unitary operations.

Additionally, we relax the aforementioned generalized parity structure of the binomial codes and numerically obtain codes with even lower unrecoverable error rates and smaller average photon number. Interestingly, some of these *numerically optimized* photonic codes can be expressed in closed form.

2 New classes of photonic codes

Suppose that flying quantum information is subjected to a error/noise channel $\mathcal{E}_\gamma$ that can be expanded in a small parameter $\gamma \ll 1$. The goal of quantum error correction is to find an encoding (denoted by projection P) and a recovery operation $\mathcal{R}$ such that the effect of the error is suppressed to some higher order L after application of the recovery:

$$\rho = P\rho P \longrightarrow \mathcal{R}\mathcal{E}_\gamma(\rho) = \rho + O\left(\gamma^{L+1}\right) . \tag{1}$$

For many physical error channels acting on multi-qubit systems, the γ-expansion of the error channel's Kraus operators consists of sums of products of single-qubit Pauli operators whose weight increases with the order in γ [10]. If the first few terms in the expansion take the code states to distinct subspaces of orthogonal error states, then those terms are correctable and the corresponding order in γ is suppressed after recovery. Quantitatively, this is represented by the Knill-Laflamme quantum error correction conditions [11]. For example, a pair of elements $\{E_1, E_2\}$ in the expansion of $\mathcal{E}_\gamma$ is correctable if and only if

$$PE_k^\dagger E_\ell P = c_{k\ell} P \tag{2}$$

for $\ell, k \in \{1, 2\}$. If the above is satisfied, then there exist syndromes which allow one to detect and correct the two corresponding errors during the recovery operation $\mathcal{R}$.

While a single mode does not consist of multiple physical qubits, we develop a similarly useful expansion in terms of the raising ($\hat{a}^\dagger$) and lowering ($\hat{a}$) operators of the mode (with $\left[\hat{a}, \hat{a}^\dagger\right] = 1$). Analogous to a multi-qubit code which protects from all single-qubit errors (i.e., operators of weight 1), there exists a binomial code which protects from single powers of $\hat{a}$ and $\hat{a}^\dagger$. We can also carry

*valbert4@gmail.com

over the principle of superposition that is so prominent in multi-qubit error correction.

2.1 Binomial codes: simple example

A simple example of the above framework is the smallest binomial code

$$|W_\uparrow\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |4\rangle\right) \qquad \text{and} \qquad |W_\downarrow\rangle = |2\rangle\,, \quad (3)$$

where $|n\rangle$ with $n \geq 0$ are the photonic Fock states. This code protects either against the pair $\{I, \hat{a}\}$ or $\{I, \hat{a}^\dagger\}$, where I is the identity (i.e., no error). One readily observes that the codes consist of Fock states of even photon numbers. This *spacing* guarantees that, upon loss (or gain) of a photon, the resulting error states remain orthogonal to the code space. Upon action of $\hat{a}$ on the code states, the resulting states $\hat{a}|W_\uparrow\rangle \propto |3\rangle$ and $\hat{a}|W_\downarrow\rangle \propto |1\rangle$ are located in the odd-photon-number subspace and are thus orthogonal to the even-subspace code words. In addition, the two error states are spaced far enough to be orthogonal to each other. The corresponding syndrome used to detect a photon loss (or gain) event is simply the photon number parity $(-)^{\hat{a}^\dagger\hat{a}}$.

However, since the code space projection is $P = |W_\uparrow\rangle\langle W_\uparrow| + |W_\downarrow\rangle\langle W_\downarrow|$, quantum error correction conditions (2) also require that $\langle W_\uparrow|\hat{a}^\dagger\hat{a}|W_\uparrow\rangle = \langle W_\downarrow|\hat{a}^\dagger\hat{a}|W_\downarrow\rangle$. This condition is equivalent to the code words having the same average photon number, which can be verified by direct observation of Eq. (3). We will show this in a different way to demonstrate why the codes are named as such. Superimposing the code words yields

$$|W_\pm\rangle = \frac{1}{2}\left(|0\rangle \pm \sqrt{2}|2\rangle + |4\rangle\right)\,, \quad (4)$$

where the coefficients are square roots of the binomial coefficients "1 2 1" from the third line of Pascal's triangle. Note that in this basis, the quantum error correction conditions (2) can be proven using the binomial formula:

$$\langle W_+|\hat{a}^\dagger\hat{a}|W_\pm\rangle = \frac{1}{2}\sum_{n=0}^{2}\binom{2}{n} n\,(\pm)^n = \frac{x}{2}\frac{d}{dx}\left(1 \pm x\right)^2\Big|_{x=1}\,.$$

2.2 Binomial codes: general case

The family of binomial codes is expressed as

$$|W^{N,S}_{\uparrow/\downarrow}\rangle = \frac{1}{\sqrt{2^N}}\sum_{p\ \text{even/odd}}^{[0,N+1]}\sqrt{\binom{N+1}{p}}\,|p(S+1)\rangle\,, \quad (5)$$

with spacing $S > 0$, order $N > 0$, and p ranging from 0 to $N+1$. The example from the previous Subsection is the $N, S = 1$ case. The previous analysis and use of the binomial formula can be straightforwardly extended to show that a code space spanned by the two codewords satisfies the quantum error correction conditions (2) for all $\hat{a}^{\dagger k}\hat{a}^\ell$ such that $|k-\ell| \leq S$ and $k+\ell \leq N$. This means that any elements of the small γ expansion of the error channel $\mathcal{E}_\gamma$ which consist of a linear superposition of such $\hat{a}^{\dagger k}\hat{a}^\ell$ can be corrected. Therefore, codes at different points of the two-dimensional parameter space $\{N, S\}$ are tailored to protecting against different types of errors. Codes with $S \gg N$ protect against error channels which cause large photon losses while codes with $S = 1 \ll N$ protect against "dephasing" error channels expressible in powers of $\hat{a}^\dagger\hat{a}$.

As a real-world example, we can consider the photonic amplitude damping channel whose Kraus operators are $E_\ell = \sqrt{\frac{(1-e^{-\gamma})^\ell}{\ell!}}\,e^{-\frac{1}{2}\gamma\hat{a}^\dagger\hat{a}}\hat{a}^\ell$. For an optical fiber, the damping factor $\gamma = l/l_{\text{att}}$ with l being the length of the channel and l_{att} being the attenuation length. For a stationary cavity, $\gamma = \kappa\delta t$ with δt being time and κ being the photon loss rate. The Kraus operators in the order-L expansion in γ for such a channel are of the form $\hat{a}^{\dagger k}\hat{a}^\ell$ with $k, \ell \leq L$. Therefore, setting $L = S = N$ allows one to satisfy Eqs. (1-2) and recover the information to the desired order.

2.3 Numerically optimized codes

The spacing between binomial code words which provides correction against photon losses comes at a price — an average photon number increasing linearly with S. We have used several numerical schemes which utilize the quantum error conditions (2) for the first few powers of $\hat{a}$ and obtained codes which do not have a spacing, have a smaller average photon number, and still correct against the chosen errors to the desired order. Surprisingly, some of these codes can be obtained analytically. For example, the code

$$\begin{aligned} |W_\uparrow\rangle &= \tfrac{1}{\sqrt{6}}\left(\sqrt{7-\sqrt{17}}|0\rangle + \sqrt{\sqrt{17}-1}|3\rangle\right) \\ |W_\downarrow\rangle &= \tfrac{1}{\sqrt{6}}\left(\sqrt{9-\sqrt{17}}|2\rangle - \sqrt{\sqrt{17}-3}|4\rangle\right) \end{aligned} \quad (6)$$

has an average photon number of approximately 1.56, compared to 2 for the smallest binomial code (3). A careful calculation ([8], Appx. H) reveals that this code is capable of correcting errors to first order in the γ-expansion of the amplitude damping channel.

3 Outlook

With the advent of binomial and numerically optimized codes in addition to the existing GKP and cat code families, there are currently (at least) four families of single-mode encodings. This raises the question: *Which encoding is best?* Expanding in the small parameters of the channel may not be sufficient to answer this question since there are many other degrees of freedom not taken into account. These include the average photon number, the employed recovery channel $\mathcal{R}$, fidelity metric, and overall experimental feasibility. In the case of GKP codes, another obstacle is the error model: those codes have not yet been thoroughly analyzed in terms of the photon loss and creation operators $\hat{a}$ and $\hat{a}^\dagger$. An implementation-independent appraisal of the various codes could begin by making use of channel-adapted quantum error recovery [12, 13]. A comparison of the best case recovery fidelities for the various codes should prove helpful in determining code applicability to various error channels.

Acknowledgments

We are grateful for useful discussions with Huaixiu Zheng, Reinier W. Heeres, Philip Reinhold, Hendrik Meier, Linshu Li, John Preskill, N. Read, Konrad W. Lehnert, Mazyar Mirrahimi, Barbara M. Terhal, Michel H. Devoret and Robert J. Schoelkopf. We acknowledge support from ARL-CDQI, ARO W911NF-14-1-0011, W911NF- 14-1-0563, NSF DMR-1301798, DGE-1122492, AFOSR MURI FA9550-14-1-0052, FA9550-14-1-0015, Alfred P. Sloan Foundation BR2013-049, and the Packard Foundation 2013-39273.

References

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Quantum cryptography,* Rev. Mod. Phys. **74**, 145 (2002).

[2] N. J. Cerf, G. Leuchs, and E. S. Polzik, *Quantum Information with Continuous Variables of Atoms and Light* (World Scientific, London, 2007).

[3] D. W. Leung, M. A. Nielsen, I. L. Chuang, and Y. Yamamoto, *Approximate quantum error correction can lead to better codes,* Phys. Rev. A **56**, 2567 (1997).

[4] D. Gottesman, A. Yu. Kitaev, and J. Preskill, *Encoding a qubit in an oscillator,* Phys. Rev. A **64**, 012310 (2001).

[5] D. Gottesman and J. Preskill, *Secure quantum key distribution using squeezed states,* Phys. Rev. A **63**, 022309 (2001).

[6] Z. Leghtas, G. Kirchmair, B. Vlastakis, R. J. Schoelkopf, M. H. Devoret, and M. Mirrahimi, *Hardware-Efficient Autonomous Quantum Memory Protection,* Phys. Rev. Lett. **111**, 120501 (2013).

[7] M. Mirrahimi, Z. Leghtas, V. V. Albert, S. Touzard, R. J. Schoelkopf, L. Jiang, and M. H. Devoret, *Dynamically protected cat-qubits: a new paradigm for universal quantum computation,* New J. Phys. **16**, 045014 (2014).

[8] M. H. Michael, M. Silveri, R. T. Brierley, V. V. Albert, J. Salmilehto, L. Jiang, and S. M. Girvin, *New Class of Quantum Error-Correcting Codes for a Bosonic Mode,* Phys. Rev. X **6**, 031006 (2016).

[9] N. Ofek, A. Petrenko, R. Heeres, P. Reinhold, Z. Leghtas, B. Vlastakis, Y. Liu, L. Frunzio, S. M. Girvin, L. Jiang, M. Mirrahimi, M. H. Devoret, and R. J. Schoelkopf, *Demonstrating Quantum Error Correction that Extends the Lifetime of Quantum Information,* arXiv:1602.04768 .

[10] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2011).

[11] E. Knill and R. Laflamme, *Theory of quantum error-correcting codes,* Phys. Rev. A **55**, 900 (1997).

[12] A. S. Fletcher, *Channel-Adapted Quantum Error Correction*, Ph.D. thesis (2007), arXiv:0706.3400 .

[13] A. S. Fletcher, P. W. Shor, and M. Z. Win, *Optimum quantum error recovery using semidefinite programming,* Phys. Rev. A **75**, 012338 (2007).

Entanglement-Assisted Quantum Communication Beating the Quantum Singleton Bound

Markus Grassl[1*]

[1] *Max-Planck-Institut für die Physik des Lichts, Günther-Scharowsky-Straße 1, Bau 24, 91058 Erlangen, Germany*

Abstract. Brun, Devetak, and Hsieh [Science **314**, 436 (2006)] demonstrated that pre-shared entanglement between sender and receiver enables quantum communication protocols that have better parameters than schemes without the assistance of entanglement. Subsequently, the same authors derived a version of the so-called quantum Singleton bound that relates the parameters of the entanglement-assisted quantum-error correcting codes proposed by them. We present a new entanglement-assisted quantum communication scheme with parameters violating this bound in certain ranges.

Keywords: Entanglement-assisted communication, teleportation, quantum codes

1 Introduction

Entanglement is a resource that enables or enhances many tasks in quantum communication. When sender and receiver share a maximally entangled state, quantum teleportation allows the sender to transmit an unknown quantum state by just sending a finite amount of classical information over a noiseless classical channel [1]. Brun, Devetak, and Hsieh [3] showed that the performance of quantum error-correcting codes (QECCs) in a communication scenario can be improved when a noisy quantum channel is assisted by entanglement.

We present a quantum communication scheme that also uses a noisy quantum channel assisted by entanglement. The main idea it to execute a teleportation protocol [1] in which the classical information is protected using a code and then sent via the noisy quantum channel to the receiver. This allows to use classical error-correcting codes. In some range, our scheme has better parameters than the one proposed in [3], showing that the adaption of the quantum Singleton bound to that class of codes presented in [4] can be violated.

2 Quantum Error-Correcting Codes

A standard quantum error-correcting code $\mathcal{C}$ of length n is a subspace of the Hilbert space $(\mathbb{C}^q)^{\otimes n}$ of n qudits. Usually, q is assumed to be a power of a prime, i.e., $q = p^m$ for some prime p. A QECC encoding k qudits has dimension q^k and is denoted by $[\![n, k, d]\!]_q$. A QECC with minimum distance $d = 2t + 1$ allows to correct all errors affecting no more than t of the subsystems. The parameters of a QECC are constraint by the so-called quantum Singleton bound [5, 6]

$$2d \leq n - k + 2. \tag{1}$$

Codes meeting this bound with equality are called *quantum MDS (QMDS) codes*.

An entanglement assisted quantum error-correcting code (EAQECC), denoted by $[\![n, k, d; c]\!]_q$, is a quantum error-correcting code that additionally uses c maximally entangled states.

*markus.grassl@mpl.mpg.de

In [4], the authors formulated a Singleton bound for the parameters $[\![n, k, d; c]\!]_q$ of an EAQECC:

$$2d \leq n - k + 2 + c. \tag{2}$$

In [3], a construction of EAQECC from any linear code $[n, \kappa, d]_{q^2}$ over the finite field $\mathbb{F}_{q^2}$ of size q^2 was given. The parameters of the resulting EAQECC are $[\![n, 2\kappa - n + c, d; c]\!]_q$, where the number c of maximally entangled states depends on the classical code and is at most $n - \kappa$. Using a classical MDS code $[n, \kappa, n-\kappa+1]_{q^2}$, we obtain an EAQECC with parameters $[\![n, k, \frac{n-k+c}{2} + 1; c]\!]_q$, meeting the bound (2) with equality when $n = k + c$ is even. Assuming the maximal value for $c = n - k$, the minimum distance of an EAQECC from this construction obeys the bound

$$d \leq n - k + 1. \tag{3}$$

which is exactly the Singleton bound for classical codes. The bound (3) is also a trivial absolute bound on the minimum distance of any quantum code.

3 The New Scheme

In our scheme, we use the c maximally entangled states in a teleportation protocol to transmit $k = c$ qudits. Each generalized Bell measurement in the teleportation protocol has q^2 possible outcomes, i.e., we have to send a classical string with $2k$ symbols from an alphabet of size q to the receiver. As we allow for n uses of a quantum channel, we can use a classical code C over an alphabet of size q encoding $2k$ symbols into n symbols, denoted by $[n, 2k, d]_q$, were again d denotes the minimum distance of the code. The classical string of length n is mapped to one of the q^n basis states of the Hilbert space of n qudits and then sent via the noisy quantum channel $\mathcal{N}$ to the receiver. The receiver measures the output of the quantum channel in the computational basis and obtains a classical string of length n. Applying error correction for the classical code C, the $2k$ symbols corresponding to the measurement results from the teleportation protocol are retrieved. The measurement and the classical decoder are depicted together as a quantum-to-classical map $\mathcal{D}_{q\to c}$ in Fig. 1. The receiver applies the corresponding correction

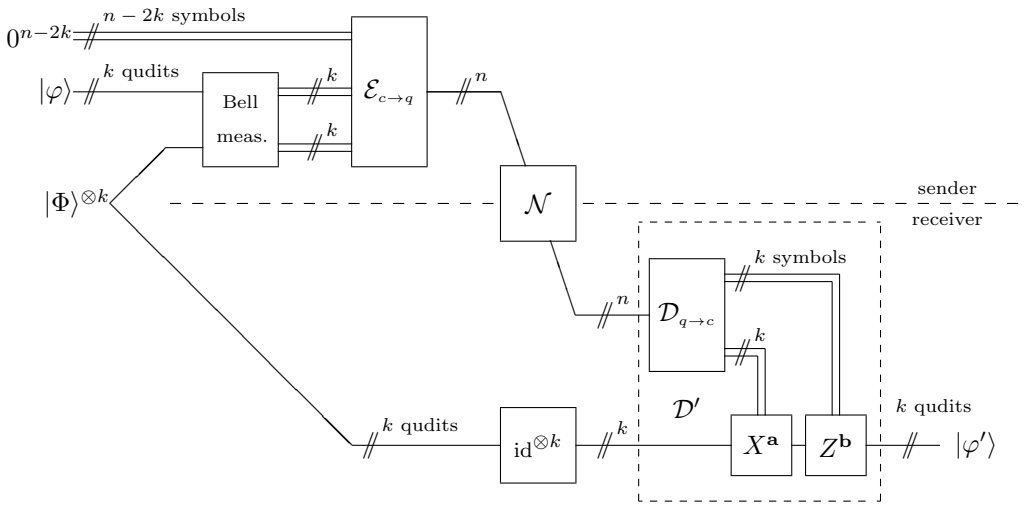


Figure 1: Our teleportation-based scheme using $c = k$ maximally entangled states.

operators $X^{\mathbf{a}}$ and $Z^{\mathbf{b}}$ to the c qudits from the c maximally entangled states and completes the teleportation protocol.

Note that we are only transmitting basis states over the quantum channel, and therefore the protocol is resilient to arbitrary phase errors. When following the standard teleportation protocol, one can replace the quantum channel by a classical channel.

The parameters of our scheme are determined by the classical code C. The Singleton bound for classical codes implies the bound

$$d \leq n - 2k + 1 \tag{4}$$

on the minimum distance of our scheme. It can be achieved whenever the classical code is an MDS code. In the special case $k = c$, the bound (2) implies

$$d \leq n/2 + 1. \tag{5}$$

Hence, for $k < n/4$ the bound (2) is more restrictive than the bound for our scheme (see also Fig. 2). Even when more maximally entangled states are used in the original construction of EAQECCs, our scheme has a larger normalized minimum distance $\delta = d/n$ for a rate $R = k/n$ below a certain threshold (e.g., $R < 1/5$ for $c = (n-k)/2$).

4 Discussion

Quantum codes based on teleportation have been considered before when studying the entanglement-assisted capacity of quantum channels [2, Section III.E]. It was observed that this results in an entanglement-assisted capacity that is half the classical capacity of the unassisted quantum channel. We are, however, not aware of related results for the finite-length case.

Our scheme beats the quantum Singleton bound (2) for quantum communication schemes with a rate below a certain threshold and uses a smaller amount c of entanglement than the scheme proposed in [3]. On the other hand, when the amount of additional entanglement does not matter, using $c = n - k$ maximally entangled in the

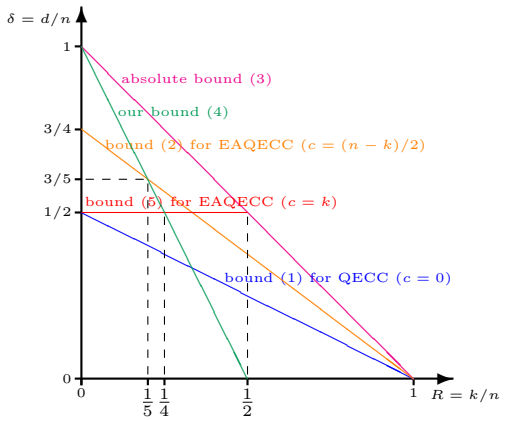


Figure 2: Asymptotic bounds (length $n \to \infty$) on the normalized minimum distance $\delta = d/n$ as a function of the code rate $R = k/n$.

original scheme has the potential to reach the absolute bound (3). It is plausible to assume that using $c > n - k$ maximally entangled states would not result in better parameters, as in this case the encoding operation $\mathcal{E}$ would map $k + c > n$ qudits to a smaller number of qubits.

Tight upper and lower bounds relating length n, dimension k, minimum distance d, and the number c of maximally entangled states have yet to be found.

References

[1] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Letters*, 70(5798):1895–1899, 1993.

[2] G. Bowen. Entanglement required in achieving entanglement-assisted channel capacities. *Phys. Rev. A*, 66(6):052313, 2002.

[3] T. Brun, I. Devetak, and M.-H. Hsieh. Correcting quantum errors with entanglement. *Science*, 314(5798):436–439, 2006.

[4] T. Brun, I. Devetak, and M.-H. Hsieh. Catalytic quantum error correction. *IEEE Trans. Inf. Theory*, 60(6):3073–3089, 2014.

[5] E. Knill and R. Laflamme. Theory of quantum error-correcting codes. *Phys. Rev. A*, 55(6):900–911, 1997.

[6] E. M. Rains. Nonbinary quantum codes. *IEEE Trans. Inf. Theory*, 45(6):1827–1832, 1999.

Symmetry-protected topologically ordered states for universal quantum computation

Hendrik Poulsen Nautrup[1] * Tzu-Chieh Wei[2] †

[1] *Institut für Theoretische Physik, Universität Innsbruck, Technikerstr. 25, A-6020 Innsbruck, Austria*
[2] *C.N. Yang Institute for Theoretical Physics and Department of Physics and Astronomy, Stony Brook University, Stony Brook, NY 11794, United States*

Abstract. Measurement-based quantum computation utilizes local measurements on suitably entangled resource states for the implementation of quantum gates. But a complete characterization for universal resource states is still missing. Motivated by the connection between symmetry-protected topological order in one dimension and the protection of certain quantum gates in measurement-based quantum computation, we show that the two-dimensional plaquette states on arbitrary lattices exhibit nontrivial symmetry-protected topological order and that they are universal resource states for quantum computation.

Keywords: measurement-based quantum computation, universal resource states, valence-bond states, quantum phases of matter, symmetry-protected topological order

1 Introduction

An intriguing connection between the resourcefulness in measurement-based quantum computation (MBQC) and certain phases of matter was discovered by Else et al. in Ref. [1], where the authors show that there exists a property of many-body states, namely symmetry-protected topological (SPT) order in one dimension, that can be utilized for the protection of certain one-qubit quantum gates in MBQC. In Ref. [2, 3] the utility of SPT phases for quantum computation in 1D has also been demonstrated for other symmetry groups beyond the $Z_2 \times Z_2$ symmetry originally considered in Ref. [1]. However, in order for quantum computation to be universal in MBQC, the entangled resource states need to be at least two-dimensional. Therefore, one important question that arises is whether there exist two-dimensional SPT states that enable universal MBQC. Moreover, if such states exist, can universality be a global property of its entire phase? Can such a state possess robustness against noise that respects the symmetry of the SPT phase? Such robustness could originate from the underlying topological nature: a symmetry-protected topologically ordered state in the presence of noise that respects a certain symmetry does not immediately undergo a quantum phase transition, i.e. it remains a gapped ground state of some generic, symmetric Hamiltonian.

2 Main Results

In our paper [4], we demonstrate that certain canonical 2D SPT tensor-network states (protected by any symmetry) indeed serve as universal resource for MBQC. These fixed point wave functions were constructed by Chen and collaborators [5, 6] using group cohomology.

The authors of Refs. [5, 6] discovered a consistent relation between the third group cohomology $\mathcal{H}^3(G, U(1))$ of a symmetry group G and SPT order in (2+1)D bosonic systems and beyond. Particularly, they prove that each nontrivial element of the third group cohomology corresponds to a distinct, nontrivial SPT phase and as such serves as a classification of SPT order. Specifically, in Ref. [6], they discuss a fixed point wave function in a canonical form, showing that it exhibits nontrivial SPT order with respect to symmetry representations constructed from nontrivial elements in $\mathcal{H}^3(G, U(1))$.

In Ref. [6] the authors predominantly considered 2D fixed-point wave functions on square and triangular lattices. Essentially, these ground states possess plaquette-like entanglement structures, built upon products of qudit GHZ-like states:

$$|\psi_{gs}\rangle = \bigotimes_j |\psi\rangle_{p_j}$$
$$= \frac{1}{d^{n_p/2}} \bigotimes_{\mathrm{j}} \left(\sum_{g=0}^{d-1} |\alpha_1 = g, \beta_2 = g, ..., \zeta_k = g\rangle_{p_j} \right)$$

where qudits within the jth plaquette p_j are labeled by $\alpha_1, \beta_2, ..., \zeta_k$.

We show that the canonical plaquette-like entanglement structures defined on arbitrary random lattices (including all regular and quasicrystalline lattices as special cases) do indeed display nontrivial SPT order while also enabling universal MBQC provided the underlying graphs are 'percolated' or, said equivalently, in the supercritical phase of percolation.

Our results show that nontrivial 2D (or higher) SPT order can give rise to universal quantum computation, strengthening the link uncovered in the 1D case by Else et al. [1]. Even though the results hold only for fixed-point wave functions, it is likely that small deformations preserving the symmetry should extend this universality to a finite region within the phase.

We note that there is a related work by Miller and Miyake [7] where they constructed a specific 2D spin-1/2 ground state respecting Z_2^3 symmetry such that it can yield random cluster states that are universal.

*hendrik.poulsen-nautrup@uibk.ac.at
†tzu-chieh.wei@stonybrook.edu

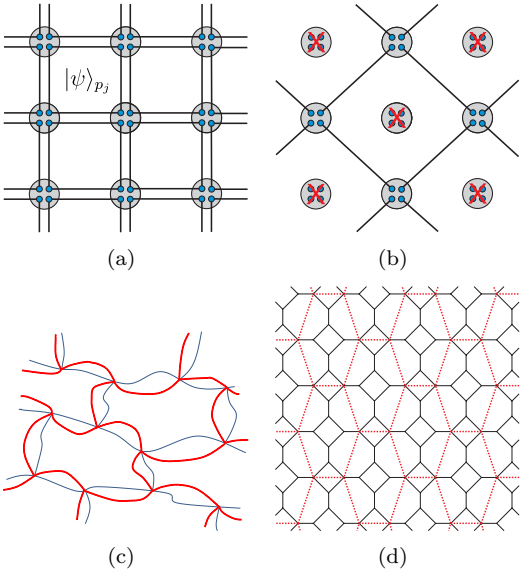


Figure 1: (a) A two-dimensional plaquette states $|\psi\rangle_{p_j}$ defined on a square lattice (blue dots: parton qudits; physical sites: shaded circles). Connections indicate entanglement. (b) Measurement reduces the plaquette state to a bond state. Red crosses mark sites on which all virtual qudits are measured in the generalized Pauli-X basis. (c) Schematic for the proof that plaquette states on arbitrary lattices are universal resources. (d) An application of (c) on the square-octagon lattice.

3 Quantum Computational Universality

The detailed proof of why the generalized plaquette states possess SPT order follows closely that of Ref. [6] by examining the symmetry action on the boundary and relating the obstruction of being a product of local unitaries to a nontrivial element in the cohomology group. Instead, we will focus on the quantum computational universality of such fixed point states.

In Fig. 1(c), we provide a schematic illustration for the proof that plaquette states on arbitrary lattices are universal resources. Essentially, using entanglement concentration from GHZ-like states to Bell-like states, we can concentrate entanglement to two parton qudits across polygons, at the expense of measuring some other qudits. The sites carrying endpoints of the resulting Bell entanglement are chosen to form vertices of a honeycomb-like subgraph. The red dashed lines depicted in Fig. 1(c) and 1(d) represent 'Bell-state'-like entanglement or 'valence-bonds' shared between parton qudits associated with some polygons. We can intuitively see that as long as the original lattice or graph has ample connectivity, the paths of the honeycomb subgraph can be chosen sufficiently far apart such that red dashed lines of two-qudit shared entanglement do not cross, and can only converge at vertices. Altogether, the resulting entanglement structure is that of a valence-bond solid as introduced by Verstraete and Cirac in Ref. [8]. Therein, valence-bond solids were also shown to be universal for MBQC. Fig. 1(b) shows the valence-bond

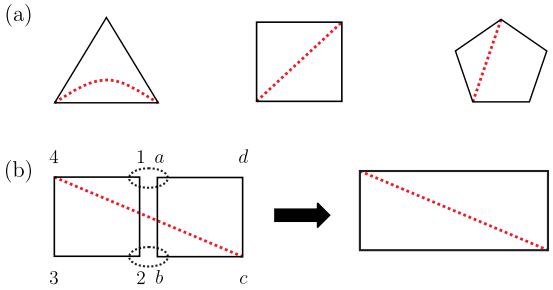


Figure 2: Illustration of entanglement concentration. (a) is an entanglement concentration to any two partons on the plaquette by measuring qudits outside the red path in the generalized Pauli-X basis. Operation in (b) merges two plaquettes into one utilizing Bell-measurements such that entanglement can be concentrated to any two partons on these two plaquettes via (a).

state obtained from the square-lattice plaquette state in Fig. 1(a). Fig. 1(d) displays an application of the general idea as described in the previous paragraph and illustrated in Fig. 1(c). Note that separation between paths does not need to be very far although we require this for the general proof of universality. (The specific tool is the entanglement concentration illustrated in Fig. 2.)

References

[1] D. V. Else, I. Schwarz, S. D. Bartlett, and A. C. Doherty. Symmetry-protected phases for measurement-based quantum computation. Phys. Rev. Lett. **108**, 240505 (2012).

[2] J. Miller, A. Miyake. Resource Quality of a Symmetry-Protected Topologically Ordered Phase for Quantum Computation. Phys. Rev. Lett. **114**, 120506 (2015).

[3] A. Prakash and T.-C. Wei. Ground states of one-dimensional symmetry-protected topological phases and their utility as resource states for quantum computation", Phys. Rev. A **92**, 022310 (2015).

[4] H. Poulsen Nautrup, T.-C. Wei. Symmetry-protected topologically ordered states for universal quantum computation. Phys. Rev. A **92**, 052309 (2015).

[5] X. Chen, Z.-C. Gu, Z.-X. Liu, and X.-G. Wen. Symmetry-Protected Topological Orders in Interacting Bosonic Systems. Science **338**, 1604 (2012).

[6] X. Chen, Y.-C. Gu, Z.-X. Liu, and X.-G. Wen. Symmetry protected topological orders and the group cohomology of their symmetry group. Phys. Rev. B **87**, 155114 (2013).

[7] J. Miller and A. Miyake. Hierarchy of universal entanglement in 2D measurement-based quantum computation. arXiv:1508.02695.

[8] F. Verstraete and J. I. Cirac Valence-bond states for quantum computation. Phys. Rev. A **70** 060302(R) (2004).

Universal Quantum Computing with Arbitrary Continuous-Variable Encoding

Hoi-Kwan Lau[1] * Martin B. Plenio[1]

[1] *Institute of Theoretical Physics, Ulm University, Albert-Einstein-Allee 11, 89069 Ulm, Germany*

Abstract. Implementing a qubit quantum computer in continuous-variable systems conventionally requires the engineering of specific interactions according to the encoding basis states. In this work, we present a unified formalism to conduct universal quantum computation with a fixed set of operations but arbitrary encoding. By storing a qubit in the parity of two or four qumodes, all computing processes can be implemented by basis state preparations, continuous-variable exponential-swap operations, and swap-tests. Our formalism inherits the advantages that the quantum information is decoupled from collective noise, and logical qubits with different encodings can be brought to interact without decoding. We also propose a possible implementation of the required operations by using interactions that are available in a variety of continuous-variable systems. Our work separates the 'hardware' problem of engineering quantum-computing-universal interactions, from the 'software' problem of designing encodings for specific purposes. The development of quantum computer architecture could hence be simplified.

Keywords: Continuous variable, quantum computer, hybrid quantum system, decoherence free subsystem

1 Introduction

In a wide range of quantum computational tasks, the basic quantity of quantum information is a two-level system that can be prepared in an arbitrary superposition state (qubit). If the quantum system consists of individually addressable energy eigenstates, such as the internal levels in trapped atoms or the polarisation states of electron spins [1], the qubit bases are most trivially represented by two of such states. On the other hand, there are also quantum systems, such as optical modes, mechanical oscillators, quantised motion of trapped ions, and spin ensembles [2, 3, 4, 5, 6], that consist of an abundance of evenly-spaced energy levels. In these systems, usually referred to as continuous-variable (CV) systems, addressing a particular energy eigenstate is usually challenging. There is thus no trivial CV representation of a qubit.

Nevertheless, the large Hilbert space of each degree of freedom, usually called a quantum mode (qumode), provides the flexibility for designing qubit encodings. Each popular encoding has its own strength and drawbacks. For instances, Fock state encoding [7, 8, 9] and coherent state encoding [10, 11] enable efficient state preparation and linear-optical logic gates, but some logic gates are probabilistic and their implementations require stringent detection efficiencies. Cat state encoding enables quantum error correction against photon loss [12, 13], but implementing the logic gates may require slow Zeno dynamics. The Gottesman-Kitaev-Preskill (GKP) protocol enables fault-tolerant quantum computating and logical states to be readout by accurate homodyne detection, but the basis states are superpositions of squeezed states which the construction is technically challenging [14, 15].

Conventionally, implementing the computing logical processes requires the engineering of dedicated interactions according to the characteristics of the encoding basis, which may require a specific physical setup, i.e. hardware, that cannot be changed as easily as the choice of encoding. For example, the phase-shift gate for the Fock state encoding, i.e., $|0_L\rangle = |0\rangle$ and $|1_L\rangle = \hat{a}^\dagger|0\rangle$, is implemented by applying the operation $\exp(i\phi\hat{a}^\dagger\hat{a})$. However, this operation does not implement a logical phase-shift, but it maps the state out of the computational subspace for coherent state encoding, i.e., $|0_L\rangle = |\alpha\rangle$ and $|1_L\rangle = |-\alpha\rangle$. The variety of encoding diversifies the architecture of CV quantum computers, and precludes the strengths of each encoding to be shared with all others.

We ask a question, is there a unified scheme that could conduct universal quantum computation irrespective of the basis states? The answer is, surprisingly, yes. In our work, we describe two universal quantum computing schemes that all logical processes are independent of the encoding state in each qumode. Specifically, a qubit is stored in the parity of two or four qumodes. The logical processes, which include computational state initialisation, universal set of logic gates, and state-readout, can be implemented by the preparation of encoding basis states $|0_L\rangle$ and $|1_L\rangle$, exponential-swap operations, i.e., $e^{i\theta\hat{S}}|\psi_1\rangle|\psi_2\rangle = \cos\theta|\psi_1\rangle|\psi_2\rangle + i\sin\theta|\psi_2\rangle|\psi_1\rangle$, and swap-tests [16]. We also show how the required operations can be implemented with realistic CV interactions that could be found in superconducting cavity QED systems, mechanical oscillator systems, and trapped ions.

Our work separates the 'hardware' problem of engineering quantum-computing-universal interactions, from the 'software' problem of designing encodings for specific purposes. The development of quantum computer architecture could hence be simplified. Additionally, the schemes also come with two advantages. First, they inherently allow logical qubits with different encoding to be brought to interact without decoding. This unprecedented flexibility would allow the strengths of different encodings to be utilised in the same computation, when each encoding is employed in the computational

*hklau.physics@gmail.com

process that it is best adopted. For instance, coherent states are efficiently created as undetected logical ancillae, cat states are best for transmitting quantum information through lossy links, and the final result is accurately readout from GKP qubits.

Second, the logical states are robust against collective noise. In CV quantum computation, leakage error is a major form of error as the environmental noise typically projects the encoded state out of the computational subspace. In some CV systems, the noise is the same in each qumode. The decoherence effect of such collective noise can be reduced by storing the quantum information in the decoherence-free-subsystem (DFS) [17, 18, 19]. As a merit of our schemes, the logical states are inherently within the DFS. The key idea is that collective noise commutes with the swap operation, which is the foundation of the logical processes. To the best of our knowledge, our schemes are also the first explicit protocols that incorporate DFS in CV systems.

More details of our work can be found in the arXiv posting [20].

References

[1] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, J. L. O'brien. Quantum Computers. Nature **464**, 45–53 (2010)

[2] S. L. Braunstein and P. van Loock. Quantum information with continuous variables. Reviews of Modern Physics **77**, 513–577 (2005)

[3] Menno Poot and Herre S. J. van der Zant. Mechanical systems in the quantum regime. Physics Reports **511**, 273–335 (2012)

[4] H. Häffner, C. F. Roos, R. Blatt. Quantum computing with trapped ions. Physics Reports **469**, 155–203 (2008)

[5] Karl Tordrup, Antonio Negretti, Klaus Mølmer. Holographic Quantum Computing. Physical Review Letters **4**, 040501 (2008)

[6] J. Wesenberg, A. Ardavan, G. Briggs, J. Morton, R. Schoelkopf, D. Schuster, K. Mølmer. Quantum Computing with an Electron Spin Ensemble. Physical Review Letters **103**, 070502 (2009)

[7] I. L. Chuang and Y. Yamamoto. Simple Quantum Computer. Physical Review A **52**, 3489–3496 (1995)

[8] I. L. Chuang and Y. Yamamoto. The persistent qubit. quant-ph/9604030, 1997.

[9] E. Knill, R. Laflamme, G. J. Milburn. A scheme for efficient quantum computation with linear optics. Nature **409**, 46–52 (2001)

[10] T. C. Ralph, A. Gilchrist, G. J. Milburn, W. J. Munro, S. Glancy. Quantum computation with optical coherent states. Physical Review A **68**, 042319 (2003)

[11] A. P. Lund, T. C. Ralph, H. L. Haselgrove. Fault-tolerant linear optical quantum computing with small-amplitude coherent states. Physical Review Letters **100**, 030503 (2008)

[12] Zaki Leghtas, Gerhard Kirchmair, Brian Vlastakis, Robert J. Schoelkopf, Michel H. Devoret, Mazyar Mirrahimi. Hardware-Efficient Autonomous Quantum Memory Protection. Physical Review Letters **111**, 120501 (2013)

[13] Mazyar Mirrahimi, Zaki Leghtas, Victor V. Albert, Steven Touzard, Robert J. Schoelkopf, Liang Jiang, Michel H. Devoret. Dynamically protected cat-qubits: a new paradigm for universal quantum computation. New Journal of Physics **16**, 045014 (2014)

[14] D. Gottesman, A. Kitaev, J. Preskill. Encoding a qubit in an oscillator. Physical Review A **64**, 012310 (2001)

[15] Nicolas C. Menicucci Fault-Tolerant Measurement-Based Quantum Computing with Continuous-Variable Cluster States. Physical Review Letters **112**, 120504 (2014)

[16] Radim Filip Overlap and entanglement-witness measurements. Physical Review A **65**, 062320 (2002)

[17] E. Knill, R. Laflamme, L. Viola, L Theory of quantum error correction for general noise. Physical Review Letters **84**, 2525–2528 (2000)

[18] P. Zanardi Stabilizing quantum information. Physical Review A **63**, 012301 (2001)

[19] J. Kempe, D. Bacon, D. A. Lidar, K. B. Whaley Theory of decoherence-free fault-tolerant universal quantum computation. Physical Review A **63**, 042307 (2001)

[20] Hoi-Kwan Lau and Martin B. Plenio. Universal Quantum Computing with Arbitrary Continuous-Variable Encoding. quant-ph/1605.09278, 2016.

Measurement-based quantum computation with mechanical oscillators

A. Ferraro[1] * O. Houhou[2] D. Moore[1] M. Paternostro[1] T. Tufarelli[3]

[1] *School of Mathematics and Physics, Queens University, Belfast BT7 1NN, United Kingdom*
[2] *Laboratoire de Physique Mathématique et Subatomique (LPMS), Université de Constantine 1, Constantine, Algeria*
[3] *School of Mathematical Sciences, University of Nottingham, Nottingham NG7 2RD, United Kingdom*

Abstract. It has recently been demonstrated that various types of mechanical oscillators can operate deeply in the quantum regime. We explore the possibility of using them as platforms for quantum computation over continuous variables. In particular, we consider an optomechanical system composed of a single cavity mode interacting with a set of mechanical resonators and we propose a scheme for generating the so-called cluster state, a universal resource for measurement-based quantum computation. We also introduce a tomographic method to verify the cluster generation and we detail the necessary measurements to perform arbitrary Gaussian operations.

Keywords: quantum computation, continuous variables, optomechanical systems, quantum tomography

Quantum computation over infinite-dimensional systems (continuous variables) has been historically explored focussing first on the circuit model of computation [1], much akin to finite-dimensional systems (discrete variables). However, it was soon realised that a valid alternative approach is constituted by the so called measurement-based model [2]. The latter allows to perform general processing of quantum information over continuous variables provided a suitable entangled state — dubbed *cluster state* — is used as a resource and additional measurements are locally performed over its constituents. Despite the limitations of finite squeezing, both the circuit and measurement based models have been theoretically proven to be fault tolerant, once proper encodings are introduced.

Much effort has been recently devoted towards the generation of cluster states whose nodes are constituted of light modes. On the other hand, recent experimental advances have shown that various types of massive mechanical oscillators can operate deeply in the quantum regime [3], promoting these systems to interesting candidates for quantum technologies. These achievements, together with the possibility to scale up the number of involved oscillators, pave the way for more advanced quantum information applications. In this context, Schimidt *et al.* [4] have proposed a platform, based on the linearized radiation-pressure interaction, to implement general Gaussian operations between multiple mechanical oscillators. The implementation of such a platform would represent a first step towards the realization of the circuit model of universal quantum computation over continuous variables. However, specific schemes for continuous-variable measurement-based computation involving massive degrees of freedoms, rather than radiative ones, are still lacking. The main advantage of this would be that, being hosted in stationary or solid-state based architectures, they offer a promising path towards integrated and scalable quantum technologies.

In order to bridge this gap, the aim of the present work is to introduce a scheme to generate, verify, and process information over continuous-variable cluster states of mechanical oscillators.

Generation of the cluster state over a mechanical-oscillator network— We propose a scheme for generating cluster states whose nodes are embodied by the mechanical modes of an optomechanical system. These states are obtained by properly engineering both the Hamiltonian and the dissipative dynamics of the radiation degrees of freedom. Specifically, the method we use to engineer the desired Hamiltonian is based on multi-tone external driving, adapting and generalizing previous approaches so that the required sidebands could be independently excited. In order to drive dissipatively the system to the graph states, we use a theoretical framework — introduced in Ref. [5] — that adapts quantum dissipation engineering to Gaussian continuous-variable systems. The merit of our scheme is that one can generate arbitrary

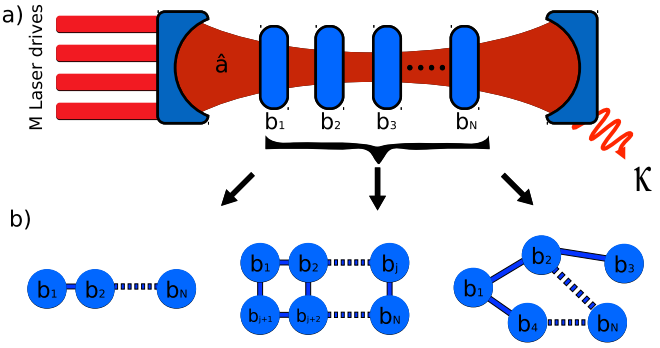


Figure 1: (Color online) (a) : An optomechanical system consisting of one optical cavity mode a coupled to N non-interacting mechanical resonators $b_1, \ldots, b_N$. The cavity dissipates with a damping rate κ, and it is driven by M classical laser fields. (b) : The state of the mechanical resonators can be prepared in different graph state geometries, *e.g.*, from left to right, a linear, a dual-rail, and a generic graph state. A graph state with lattice geometry is called cluster state and can be proven to be a universal resource for quantum computation over continuous-variable systems.

*a.ferraro@qub.ac.uk

graph states only by driving the optomechanical system with a sequence of tunable pulses. The generation protocol is sketched in Fig.1 and described in full in Ref. [6] — where the interested reader can find all the technical details, including the effect of mechanical noise.

Quantum state reconstruction of the mechanical-oscillator network— Once the cluster state has been generated, a question immediately arises: how can we verify that the state prepared in the experiment is indeed the desired one? In the language of Quantum Mechanics, the problem is that of experimentally estimating the density operator of the mechanical system. It is well known that the full information encoded in the density operator cannot be accessed through the measurement of a single observable. One must instead collect the measurement statistics of several distinct observables, a task which requires access to many copies of the quantum system of interest. By post-processing the outcomes of these measurements, the experimenter may estimate the density operator via techniques broadly known as *quantum tomography* or *quantum state reconstruction*.

In an optomechanical context various approaches to quantum state reconstruction have been explored in the literature, for example employing quantum non-demolition measurements of mechanical quadratures, using short laser pulses to prepare and read out the mechanical state, or exploiting a detuned driving field [3]. However, to the best of our knowledge, no method has been proposed for the efficient readout of the quantum state of an oscillator network in an optomechanical setting.

We propose a protocol of quantum state reconstruction for the mechanical portion of the optomechanical system used to generate the cluster state (again, see Fig. 1). Our protocol relies on the linearized radiation pressure interaction, and exploits measurements on the accessible output modes of the optical cavity. By controlling in time the interaction strength, we show that it is possible to encode information about any mechanical quadrature in the cavity mode, which can then be measured through the output field leaking out of the system. Specifically, an arbitrary moment of the selected quadrature can be estimated via appropriate light-quadrature measurements, followed by the inversion of a linear system of equations. Similarly to Ref. [7], an important advantage of this scheme is that it requires minimal access to the mechanical network, in that only one light probe is sufficient to reconstruct the state of the entire network. Details can be found in the annexed technical appendix.

Quadrature Measurements for Computation— In order to carry out a computation on the cluster state, appropriate measurements must be available to repeatedly drive the cluster step by step into the required state. For continuous-variable clusters, an arbitrary Gaussian transformation can be achieved via suitable Gaussian measurements, that can be implemented in the same set-up considered thus far.

To achieve quadrature measurements on the mechanics by monitoring the cavity field one must engineer a quantum non-demolition interaction between the desired quadrature measurement operator and the cavity field. This can be achieved by modulating the driving fields with the appropriate mechanical frequency, while the phase of this modulation determines which quadrature is addressed. Continuous measurements are then carried out on the cavity field via homodyne detection. Tracking the evolution of the mechanical system shows that, when this indirect measurement is performed on a node of the cluster state, the steady state of the remaining nodes transforms as for the case of a strong projective measurement. One can show that the procedure is robust when noise in the measurement is included. This implies that any single-mode mechanical measurement can be performed by measuring the cavity field only, allowing in turn the realisation of arbitrary Gaussian dynamics over the cluster.

In summary, our work shows that a cavity-optomechanics set-up allows for the generation and verification of continuous-variable cluster states. In addition, the same set-up allows to perform arbitrary Gaussian operations measuring the cavity field only, which constitutes a necessary step towards universal quantum computation.

References

[1] S. L. Braunstein and P. Van Loock, "Quantum information with continuous variables," *Rev. Mod. Phys.*, vol. 77, no. 2, p. 513, 2005.

[2] C. Weedbrook, S. Pirandola, R. Garcia-Patron, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information," *Rev. Mod. Phys.*, vol. 84, no. 2, p. 621, 2012.

[3] M. Aspelmeyer, T. J. Kippenberg, and F. Marquardt, "Cavity optomechanics," *Rev. Mod. Phys.*, vol. 86, no. 4, p. 1391, 2014.

[4] M. Schmidt, M. Ludwig, and F. Marquardt, "Optomechanical circuits for nanomechanical continuous variable quantum state processing," *New J. Phys.*, vol. 14, no. 12, p. 125005, 2012.

[5] Y. Ikeda and N. Yamamoto, "Deterministic generation of gaussian pure states in a quasilocal dissipative system," *Phys. Rev. A*, vol. 87, no. 3, p. 033802, 2013.

[6] O. Houhou, H. Aissaoui, and A. Ferraro, "Generation of cluster states in optomechanical quantum systems," *Phys. Rev. A*, vol. 92, p. 063843, Dec 2015.

[7] T. Tufarelli, A. Ferraro, M. S. Kim, and S. Bose, "Reconstructing the quantum state of oscillator networks with a single qubit," *Phys. Rev. A*, vol. 85, p. 032334, Mar 2012.

Tripartite-to-bipartite entanglement transformation by stochastic local operations and classical communication and the classification of matrix spaces

Yinan Li[1] * Youming Qiao[1] † Xin Wang[1] ‡ Runyao Duan[1 2] §

[1] *Centre for Quantum Computation and Intelligent Systems (QCIS), Faculty of Engineering and Information Technology, University of Technology Sydney (UTS), NSW 2007, Australia*

[2] *UTS-AMSS Joint Research Laboratory for Quantum Computation and Quantum Information Processing, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China*

Abstract. We consider the problem of transforming a tripartite state to a bipartite state by stochastic local operations and classical communication (SLOCC). We first exhibit a family of tripartite states of which a single copy cannot be transformed to the bipartite maximally entangled state, while two copies can. We then characterize tripartite pure states of which multiple copies will have more advantages in SLOCC transformation than a single copy. Finally we explicitly compute the SLOCC distillation rate of a family of tripartite states and characterize those tripartite states which can be transformed to the bipartite maximally entangled state by SLOCC in an asymptotic setting. Our approach is based on the classification of matrix spaces according to the singularity.

Keywords: Entanglement transformation, Entanglement distillation rate, SLOCC, Maximal rank of matrix space

1 Introduction

What is the optimal number of copies of a given N-partite state $|\phi\rangle$ that can be obtained from a given N-partite state $|\psi\rangle$, when each party can only perform local operations on their respective systems with the help of unlimited two-way classical communication (LOCC)? This optimal number is named as the entanglement transformation rate. In practice, evaluating the entanglement transformation rate, especially in the multipartite case, is difficult since the class of LOCC is still not satisfactorily understood. To partially remedy this situation, we relax the restriction of LOCC and consider the class of stochastic local operations and classical communication (SLOCC). Remarkably, multipartite to bipartite SLOCC entanglement convertibility was shown to be equivalent to the polynomial identity testing (PIT) problem [1]. After that work, it is natural to consider the multipartite-to-bipartite SLOCC transformation problem. In this paper we exhibit several results in this direction.

Our results are based on the connection of this problem with the structure of matrix spaces, which was first suggested in [1]. This work was, however, heavily inspired by the recent progress on the non-commutative rational identity testing problem, settled in [2] and [3].

2 Main Results

In this paper, we focus on transforming tripartite pure state $|\psi\rangle_{ABC} \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$ where $\dim(\mathcal{H}_A) = \dim(\mathcal{H}_B) = \dim(\mathcal{H}_C) = d$, to a bipartite pure state $|\phi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$. We use ψ_{ABC} to denote the projection $|\psi\rangle\langle\psi|_{ABC}$. Define $K(\psi_{ABC}) = \max\{\mathrm{Sch}(\phi_{AB}) : |\phi\rangle_{AB} \in \mathrm{supp}(\mathrm{Tr}_{C\ ABC})\}$, where $\mathrm{Sch}(\phi_{AB})$ is the Schmidt rank of $|\phi\rangle_{AB}$. In [1], it has been shown that $|\psi\rangle_{ABC}$ can be transformed to $|\phi\rangle_{AB}$ by SLOCC if and only if $K(\psi_{ABC}) \geq \mathrm{Sch}(\phi_{AB})$.

Using the linear isomorphism $\Delta(|i\rangle \otimes |j\rangle) = |i\rangle\langle j|$, we denote $M(\psi_{ABC}) = \Delta[\mathrm{supp}(\mathrm{Tr}_C\psi_{ABC})]$, which is a linear space of matrices (a.k.a. matrix space). Equivalently, $K(\psi_{ABC}) = \mathrm{mrk}(M(\psi_{ABC})) = \max\{\mathrm{rank}(E) : E \in M(\psi_{ABC})\}$. Thus it is interesting to consider the maximal rank of a matrix space. We say a matrix space is non-singular if it contains a full rank matrix. Otherwise we say it is singular. Intuitively, only those tripartite states $|\psi\rangle_{ABC}$ such that $M(\psi_{ABC})$ is non-singular can be transformed to the bipartite maximally entangled state by SLOCC. A very important structure to witness the singularity of a matrix subspace is the shrunk subspace. A linear subspace $U \leq \mathbb{C}^d$ is called a shrunk subspace of a $d \times d$ matrix space $\mathcal{S}$ if $\dim(U) > \dim(\mathcal{S}(U))$, where $\mathcal{S}(U) = \mathrm{span}\{\cup_{E\in\mathcal{S}} EU\}$. If a matrix space has a shrunk subspace, it must be singular and we call it a shrinking matrix space. If a matrix space is neither non-singular nor shrinking, we call it exceptional (e.g. the space of 3×3 skew-symmetric matrices). In addition, We say two matrix spaces $\mathcal{S}$ and $\mathcal{S}'$ are equivalent, if there exist two invertible matrices P and Q such that $P\mathcal{S}Q = \mathcal{S}'$.

Now we will using techniques of matrix spaces to study the tripartite-to-bipartite transformation. First, we exhibit a family of tripartite states which cannot be transformed to the bipartite maximally entangled state with a single copy by SLOCC, but can do so with two copies.

Theorem 1 *Let* $|\psi^d\rangle_{ABC}$ *be a tripartite state with*

*Yinan.Li@student.uts.edu.au
†Youming.Qiao@uts.edu.au
‡Xin.Wang-8@student.uts.edu.au
§Runyao.Duan@uts.edu.au

$\mathrm{supp}(\mathrm{Tr}_C(\psi_{ABC}^d)) = \mathrm{span}\{|i\rangle|j\rangle - |j\rangle|i\rangle : 0 \le i,j \le d-1\}$. *If d is odd, we have*

$$|\psi^d\rangle_{ABC} \overset{\text{SLOCC}}{\not\longrightarrow} |\Phi_d\rangle_{AB},$$

but

$$|\psi^d\rangle_{ABC}^{\otimes 2} \overset{\text{SLOCC}}{\longrightarrow} |\Phi_d\rangle_{AB}^{\otimes 2},$$

where $|\Phi_d\rangle_{AB}$ is the d-dimensional bipartite maximally entangled state shared by A and B.

In general, we are interested in those states of which multiple copies have more advantages in SLOCC transformation than a single copy. Indeed this problem can be fully solved, as shown in the following theorem.

Theorem 2 *A tripartite state $|\psi\rangle_{ABC} \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$ satisfies $K(\psi_{ABC}^{\otimes 2}) > K(\psi_{ABC})^2$ if and only if its isometric bipartite matrix space $M(\psi_{ABC}) \le \mathcal{M}(d)$ satisfies:*

1. $\mathrm{mrk}(M(\psi_{ABC})) < \dim(\mathrm{Im}(M(\psi_{ABC})))$, *and*
2. $\mathrm{mrk}(M(\psi_{ABC})) < d - \dim(\mathrm{Ker}(M(\psi_{ABC})))$,

where $\mathrm{Ker}(\mathcal{S}) = \cap_{E\in\mathcal{S}}\mathrm{Ker}(E)$ *and* $\mathrm{Im}(\mathcal{S}) = \mathrm{span}\{\cup_{E\in\mathcal{S}}\mathrm{Im}(E)\}$.

Moreover, we consider the tripartite-to-bipartite transformation by SLOCC in an asymptotic setting. In particular, the transformation to the bipartite maximally entangled state, which can be viewed as a SLOCC entanglement distillation problem. Define the bipartite entanglement distillation rate of a tripartite state $|\psi\rangle_{ABC}$ by

$$R_D(\psi_{ABC}) = \sup\{r : |\psi\rangle_{ABC}^{\otimes n} \overset{\text{SLOCC}}{\longrightarrow} |\Phi_2\rangle_{AB}^{\otimes nr}\}.$$

By the result in [1], we have

$$\begin{aligned} R_D(\psi_{ABC}) &= \log_2 \mathrm{mrk}^\infty(M(\psi_{ABC})) \\ &= \lim_{n\to+\infty} \frac{1}{n}\log_2 \mathrm{mrk}(M(\psi_{ABC}^{\otimes n})). \end{aligned}$$

We call $\mathrm{mrk}^\infty(\mathcal{S})$ the asymptotic maximal rank of the matrix space $\mathcal{S}$. We say $|\psi\rangle_{ABC}$ can be transformed to the bipartite maximally entangled state by SLOCC asymptotically if $R_D(\psi_{ABC}) = \log_2 d$. Though it is generally difficult to calculate the bipartite entanglement distillation rate, we still have the following characterization:

Theorem 3 *$|\psi\rangle_{ABC}$ can be transformed to the bipartite maximally entangled state by SLOCC asymptotically, i.e., $\mathrm{mrk}^\infty(M(\psi_{ABC})) = d$, if and only if $M(\psi_{ABC})$ has no shrunk subspace.*

It is sufficient to consider singular matrix spaces and prove the following two cases:

- For a matrix space $\mathcal{S}$ which has a shrunk subspace, $\mathrm{mrk}^\infty(\mathcal{S}) < d$;
- For a matrix space $\mathcal{R}$ which does not have a shrunk subspace, $\mathrm{mrk}^\infty(\mathcal{R}) = d$.

For a shrinking matrix space $\mathcal{S}$, up to equivalence, it can be regarded as a subspace of a maximal compression space $\mathcal{A}(p,q,d) := \mathrm{span}\{\{|i\rangle\langle j| : 1 \le i \le p,\ 1 \le j \le d\} \cup \{|i\rangle\langle j| : p+1 \le i \le d,\ 1 \le j \le q\}\}$ with parameters (p,q,d) and $p+q<d$.

We can calculate the asymptotic maximal rank of a maximal compression space, hence the bipartite entanglement distillation rate of the associated tripartite state, by the following formula:

Theorem 4 $\log_2 \mathrm{mrk}^\infty(\mathcal{A}(p,q,d)) = \log_2 d - k$, *where* $k = \min\{D((1-\alpha)||p'), D(\alpha||q')\}$. *Here* $p' = \frac{p}{d}$, $q' = \frac{q}{d}$, $\alpha = \frac{\log_2(d-q)-\log_2 p}{\log_2((d-p)(d-q))-\log_2(pq)}$ *and* $D(a||b) = a\log_2\frac{a}{b} + (1-a)\log_2\frac{1-a}{1-b}$.

Since $D(a||b) = 0$ if and only if $a = b$. We can obtain $k > 0$. Thus for any shrinking matrix space $\mathcal{S} \le \mathcal{M}(d)$, it is a subspace of $\mathcal{A}(p,q,d)$ for some parameters (p,q,d), we have $\mathrm{mrk}^\infty(\mathcal{S}) \le \mathrm{mrk}^\infty(\mathcal{A}(p,q,d)) < d$.

On the other hand, for matrix spaces $\mathcal{R}_1, \mathcal{R}_2 \le \mathcal{M}(d)$ which have no shrunk subspace, $\mathcal{R}_1 \otimes \mathcal{R}_2$ still has no shrunk subspace. This can be proved by using the invariant-theoretic characterizations of shrinking matrix spaces (see e.g. [2]). In particular, we have $\frac{1}{2}d \le \mathrm{mrk}(\mathcal{R}_1) \le d$ [4]. Thus $\mathrm{mrk}^\infty(\mathcal{R}) = d$.

In addition, we have the following corollary directly obtained by the results in [2] and [3]:

Corollary 5 *There is a deterministic polynomial time algrithm to determine whether a tripartite state can be transformed to the maximally bipartite entangled state by SLOCC asymptotically.*

3 Conclusion

In summary, we use the structure of matrix spaces to study the entanglement transformation from a tripartite pure state to a bipartite pure state by SLOCC. We exhibit examples which cannot be transformed to bipartite maximally entangled state by SLOCC, while two copies can. Then we characterize those tripartite states of which multiple copies will have advantages in SLOCC entanglement transformation than a single copy. Importantly, we obtain a full characterization for those tripartite states which can be transformed to bipartite maximally entangled state by SLOCC in an asymptotical setting. In particular we exhibit a closed formula to calculate the tripartite-to-bipartite entanglement distillation rate for a large class of tripartite states.

References

[1] E. Chitambar, R. Duan, and Y. Shi, *Phys. Rev. A* **81**, 52310 (2010).

[2] G. Ivanyos, Y. Qiao, and K. V Subrahmanyam, arXiv1512.03531 (2015).

[3] A. Garg, L. Gurvits, R. Oliveira, A. Wigderson, arXiv:1511.03730 (2015).

[4] M. Fortin, C. Reutenauer. Séminaire Lotharingien de Combinatoire. 2004;52:B52f.

Information gain and disturbance in quantum measurements revisited

Francesco Buscemi[1] * Siddhartha Das[2] † Mark M. Wilde[2] ‡

[1] *Nagoya University, Furo-cho, Chikusa-ku, 460-0864, Nagoya, Japan*
[2] *Lousiana State University, Baton Rouge, Louisiana 70803, USA*

Abstract. In this work we derive some new information-theoretic bounds relating information gain and disturbance in quantum measurements. Such bounds considerably strengthen previous results and solve an open problem posed in [F. Buscemi and M. Horodecki, Open Sys. Inf. Dyn. **16**, 29 (2009)]. We do this by proving a new inequality for the entropy change in quantum channels and by specializing some recent results in the theory of approximate reversibility.

Keywords: quantum measurements, information gain, entropic disturbance, entropy gain, approximate reversibility, subunital channels

Introduction. The measurement process is central in quantum theory as it describes the observer's act of gathering information about the external world. It is quite natural then to adopt an information-theoretic viewpoint when studying quantum measurements.

To the best of our knowledge, the first attempt to explicitly characterize a quantum measurement $\mathfrak{M}$ in terms of an entropic quantity (namely, related to the von Neumann–Shannon entropy) was by the Dutch theoretical physicist Groenewold, who in 1971 introduced his *information gain*, conjecturing that it be always non-negative (thus the name "gain") [1]. We have to remind that, at that time, the only widely known model for quantum measurements was the von Neumann–Lüders projection postulate. Indeed, in such a restricted scenario, Groenewold's information gain is always non-negative (this was proved by Lindblad) but the more general theory of quantum instruments (developed in the meanwhile by Davies and Lewis and by Ozawa) makes room for quantum measurements with a *negative* information gain (this was proved by Ozawa [2]).

More recently, the problem of characterizing the information gain of a quantum measurement has been considered from the viewpoint of quantum information theory. In particular, the definition given by Groenewold has been modified so that, while it coincides with the original one in all those cases in which this is positive, it continues to remain positive also for more general quantum measurement processes (while Groenewold's measure turns negative) [3]. Moreover, such a modified information gain acquires a clear-cut operational interpretation due to Winter's quantum measurement compression protocol [4].

Information gain and entropy change. Suppose that the system being measured initially is in state ρ and that, conditional on the outcome m of the measurement, its state has correspondingly changed to σ_m. Groenewold information gain is then defined as an "average entropy reduction" due to the measurement $\mathfrak{M}$, i.e.,

$$I_G(\rho, \mathfrak{M}) \equiv H(\rho) - \sum_m p(m) H(\sigma_m),$$

where H denotes the von Neumann entropy and $p(m)$ is the probability of outcome m. Therefore, the study of Groenewold information gain amounts to the study of entropy changes.

The first result we present here is a simple yet powerful bound to the entropy change in quantum channels:

Theorem 1 ([5]) *Let Φ be a completely positive trace-preserving (CPTP) map. For any input state ρ, the following relation holds:*

$$H[\Phi(\rho)] - H(\rho) \geq D[\rho \| (\Phi^\dagger \circ \Phi)(\rho)],$$

where $\Phi^\dagger$ is the adjoint of Φ (i.e., $\mathrm{Tr}[X\ \Phi(Y)] = \mathrm{Tr}[\Phi^\dagger(Y)\ X]$ for all X and Y) and $D(X\|Y) = \mathrm{Tr}[X \log X - X \log Y]$ is the quantum relative entropy between $X \geq 0$ and $Y > 0$.

(In fact, the above statement is also true for positive, not necessarily completely positive, maps. However, for the sake of simplicity, we refrain from considering this case here, which is however of some interest in

*buscemi@is.nagoya-u.ac.jp
†sdas21@lsu.edu
‡mwilde@lsu.edu

the light of recent results generalizing the quantum data-processing inequality to positive TP maps [6].)

Here we focus in particular on an interesting consequence of Theorem 1:

Corollary 2 ([5]) *Let Φ be a CPTP map, satisfying, in particular, the condition of subunitality, i.e., $\Phi(\mathbb{1}) \leq \mathbb{1}$. Then, there exists a CPTP map Ψ such that, for any input state ρ, the following relation holds:*

$$\begin{aligned} H[\Phi(\rho)] - H(\rho) &\geq D[\rho \| (\Phi^\dagger \circ \Phi)(\rho)] \\ &\geq D[\rho \| (\Psi \circ \Phi)(\rho)] \\ &\geq 0. \end{aligned}$$

Interpreting Ψ as the *reverse channel* of Φ, the above corollary states that

1. if the entropy gain is small, then the action of Φ can be approximately undone (by Ψ);
2. if Φ is not approximately reversible (i.e., $\min_\Psi D[\rho \| (\Psi \circ \Phi)(\rho)]$ is "large") then the entropy gain too must be "large".

Application to efficient quantum measurements. Efficient quantum measurements are those such that, for each outcome m, there exists an operator E_m such that $\sigma_m = E_m \rho E_m^\dagger / \operatorname{Tr}[E_m \rho E_m^\dagger]$. In this case, the CPTP map defined by

$$\mathcal{M}(\rho) \equiv \sum_m E_m \rho E_m^\dagger \otimes |m\rangle\langle m|$$

is automatically subunital. Hence, in the case of efficient quantum measurements, Corollary 2 provides the following bound on the operational information gain I:

$$H(M) - I(\rho, \mathfrak{M}) \geq D[\rho \| (\tilde{\mathcal{M}} \circ \mathcal{M})(\rho)], \qquad (1)$$

where $H(M)$ is the Shannon entropy of the outcome distribution $p(m) = \operatorname{Tr}[E_m \rho E_m^\dagger]$ and $\tilde{\mathcal{M}}$ is the reverse of $\mathcal{M}$.

In Ref. [7], Jacobs interprets the bound

$$\Delta S \equiv H(M) - I(\rho, \mathfrak{M}) \geq 0$$

as a generalized second law for efficient quantum measurements. It is then clear that our bound (1) constitutes a *strengthened* generalized second law, in that it not only shows that ΔS is non-negative for efficient measurements (a trivial consequence of the non-negativity of the relative entropy), but also states that, whenever ΔS is "small", then the measurement process is almost reversible, as it happens in adiabatic thermodynamical processes.

Entropic disturbance. Given an input ensemble $\mathcal{E} = \{p(x), \rho_x\}$ and a CPTP map Φ, the Holevo information loss is defined as [9]

$$\Delta\chi(\mathcal{E}) \equiv \chi(\mathcal{E}) - \chi[\Phi(\mathcal{E})],$$

where $\chi(\mathcal{E}) = H(\bar{\rho}) - \sum_x p(x) H(\rho_x)$, for $\bar{\rho} = \sum_x p(x) \rho_x$, and $\Phi(\mathcal{E})$ is the output ensemble $\{p(x), \Phi(\rho_x)\}$. The techniques developed in this work allow us to prove the following theorem:

Theorem 3 ([5]) *Let Φ be a CPTP map and $\mathcal{E} = \{p(x), \rho_x\}$ an input ensemble. Then, there exists a reverse channel Ψ such that*

$$\Delta\chi(\mathcal{E}) \geq -2 \log \sum_x p(x) \sqrt{F}[\rho_x, (\Psi \circ \Phi)(\rho_x)], \quad (2)$$

where $\sqrt{F}(\rho, \sigma)$ denotes the square-root fidelity $\|\sqrt{\rho}\sqrt{\sigma}\|_1$.

References

[1] H. J. Groenewold. A problem of information gain by quantal measurements. *International Journal of Theoretical Physics*, 4(5):327–338, 1971.

[2] M. Ozawa. On information gain by quantum measurements of continuous observables. J. Math. Phys. 27, 759 (1986).

[3] F. Buscemi, M. Hayashi, and M. Horodecki. Phys. Rev. Lett. 100, 210504 (2008).

[4] A. Winter. Comm. Math. Phys. 244, 157 (2004).

[5] F. Buscemi, S. Das, and M. M. Wilde. Approximate reversibility in the context of entropy gain, information gain, and complete positivity. Phys. Rev. A **93**, 062304 (2016).

[6] A. Müller-Hermes and D. Reeb. Monotonicity of the quantum relative entropy under positive maps. arXiv:1512.06117.

[7] K. Jacobs. Second law of thermodynamics and quantum feedback control: Maxwells demon with weak measurements. Physical Review A, 80(1):012322, 2009. arXiv:0906.4146.

[8] S. Wehner, M. M. Wilde, M. P. Woods. Work and reversibility in quantum thermodynamics. arXiv:1506.08145 [quant-ph].

[9] F. Buscemi and M. Horodecki. Towards a Unified Approach to Information-Disturbance Tradeoffs in Quantum Measurements. Open Sys. Inf. Dyn. **16**, 29 (2009).

Information Broadcasting During Decoherence

Jarek K. Korbicz[1 2 *]

[1] *Faculty of Applied Physics and Mathematics, Gdańsk University of Technology, 80-233 Gdańsk*
[2] *National Quantum Information Centre in Gdańsk, 81-824 Sopot, Poland*

Abstract. I will present recent studies on information transfer during decoherence, inspired by quantum information theory. I will introduce Spectrum Broadcast Structures specific quantum state structures, responsible for an emergence of objective-like properties. I will show how they appear in several well known models of decoherence, such as the illuminated sphere model, the spin-spin model, and Quantum Brownian Motion model. The latter, being the most challenging due to explicit inclusion of self-dynamics of both the central system and the environment, shows dynamical spectrum broadcast structures, encoding a motion, rather than a single parameter.

Keywords: decoherence,broadcasting,objectivity

Quantum-to-classical transition has a been a subject of a debate and active investigation from the very beginning of quantum theory. The importance of understanding the transition mechanisms lies not only in fundamental problems like how quantum mechanics explains the observed world of everyday experience, but also in more practical questions, e.g. how to preserve quantumness. One of the multiple aspects of the problem is explaining the robust, objective nature of the observed world. As it is well known, in quantum mechanics the act of observation in general changes the state of the system, thus seemingly precluding any form of objectivity. Resolution of this apparent paradox has been the subject of, so called, quantum Darwinism theory-a refined and more realistic form of decoherence theory, where the system is indirectly observed by monitoring portions of its environment and information content of those portions is the main object of the study. Building on this theory, a deeper approach using, so called, Spectrum Broadcast Structures (SBS) has been proposed in [1]. I will first briefly review the results of [1]. The approach is based on a direct analysis of quantum states of the system and a portion of the environment, rather than on information-theoretical functions. Starting from a reasonable definition of objectivity, where, roughly speaking, multiple observers measure their portions of the environment and observe the same result without disturbing the system, the argument of [1] links it to a specific state structure, using the notion of non-disturbance proposed by Bohr. The result can be interpreted in a quantum information theory terms, showing that the process of objectification is a much weaker from of quantum state broadcasting, where only information on one observable (pointer basis) is being broadcasted.

The power of the result [1] is that it has been obtained in an abstract, model independent way. A natural question arises if SBS appear in known models of decoherence. The answer is affirmative and requires a paradigmatic shift with respect to the standard decoherence studies in that instead of analyzing a reduced state of the system only, one has to look at a joint state of the system and a portion of the environment. I will first present results on simple models, neglecting self-dynamics of the system. One of them is the emblematic model of collisional decoherence-a small dielectric sphere illuminated by photons, studied from the SBS point of view in [2]. I will introduce the basic mathematical tools for searching for SBS and then show how such structures are being dynamically formed in the course of the evolution, even if the environment is initially noisy and in a more general state than thermal. Based on the general results of [1], the formation of SBS leads to objectification of the position of the sphere. Moreover, with a help of the classical Perron-Frobenius Theorem I will show a surprising effect of how the decoherence mechanism can be used to faithfully broadcast a specific message into the environment. Next, I will briefly consider the spin-spin model, where a central spin-1/2 interacts with a bath of spins-1/2 with random interaction strengths. I will show the formation of the SBS, which here makes objective the projection of the central spin on the axis chosen by the interaction. Thus, in this simple model of qubit decoherence it not only becomes a classical bit, but its value is stored in many copies in the environment. Finally, I will move to a more realistic model where self-dynamics of both the central system and the environment is included in the description-Quantum Brownian Motion (QBM), i.e. a central oscillator interacting with a bath of oscillators. The formation of SBS in the model has been studied in [3, 4] in the approximation, where the central oscillator is massive and hence feels no recoil from the environment (apart from a renormalization of its frequency). This is the opposite regime to the one usually studied so far, where the environment is supposed to be insensitive to the system and hence Born-Markov approximation can be used. Here instead, we are interested in the information flow from the system to the environment. Assuming the environment to be discrete, with random and independently, identically distributed frequencies and with a help of various simplifications I will show the formation of SBS in the studied regime. A distinctive feature of spectrum broadcast structures in this model is that, unlike in the previous ones, they are dynamical: At any moment of time a SBS is being formed. This is due to the

*jkorbicz@mif.pg.gda.pl

explicit inclusion of the self-dynamics of the central system, which rotates the pointer basis at a time-scale of the (renormalized) self-frequency. Traces of this motion are dynamically encoded into the environment. I will show the effects of non-zero temperature of the environment-the higher the temperature the stronger the decoherence of the central oscillator but the lower the informational capacity of the environment, inhibiting formation of SBS. I will end discussing several possible development paths for the presented approach.

References

[1] R. Horodecki, J. K. Korbicz, P. Horodecki. Quantum origins of objectivity. *Phys. Rev. A* 91, 032122, 2015.

[2] J. K. Korbicz, P. Horodecki, R. Horodecki. Objectivity in a Noisy Photonic Environment Through Quantum State Information Broadcasting. *Phys. Rev. Lett.* 112, 120402, 2014.

[3] J. Tuziemski, J. K. Korbicz. Dynamical Objectivity in Quantum Brownian Motion. EPL 112, 40008, 2015.

[4] J. Tuziemski, J. K. Korbicz. Objectivisation In Simplified Quantum Brownian Motion Models. *Photonics* 2(1), 228, 2015.

Characterizing the long-term behavior of a quantum ensemble

Hao-Chung Cheng[1 2 *] Min-Hsiu Hsieh[2 †] Marco Tomamichel[3 ‡]

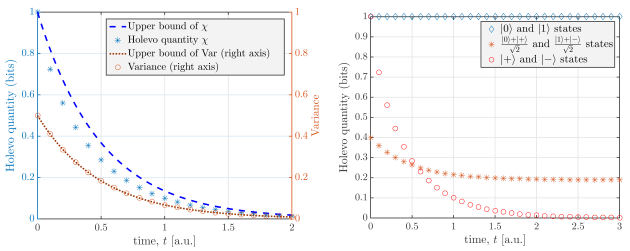
[1] *Graduate Institute Communication Engineering, National Taiwan University, Taiwan (R.O.C.)*
[2] *Centre for Quantum Computation & Intelligent Systems, Faculty of Engineering and Information Technology, University of Technology Sydney, NSW 2007, Australia*
[3] *School of Physics, The University of Sydney, NSW 2006, Australia*

Abstract. In this paper, we extend the theory of quantum Markov processes on a single quantum state to a broader theory that covers Markovian evolution of an ensemble of quantum states. This generalizes Lindblad's formulation of quantum dynamical semigroups. Our formalism includes an explicit form of semigroups, their time derivative—the infinitesimal generator, a carré du champ operator, and matrix Φ-entropy. We find a matrix Φ-Sobolev inequality that governs the exponential decay of the these matrix Φ-entropy. Special cases of the matrix Φ-entropy evaluate to the Holevo quantity and the variance of the ensemble, which allows us to relate our formalism to classical coding over quantum channels. In particular, we show that the convergence rates of two special semigroups—the depolarizing and phase-damping channels—can be explicitly computed. They result in fundamentally different equilibrium situations, for which there is no classical analogy. Our complete paper can be found in arXiv:1511.02627 [quant-ph].

Understanding the time evolution of quantum systems is a crucial problem in physics. To accurately describe the evolution of a large class of open quantum systems whose dynamics only depends on the current time step without reference to any earlier step in the sequence, a Markovian master equation is derived [1], and this forms the basis of the theory of quantum Markov processes. The formulation includes an explicit form of a quantum dynamical semigroup (QDS). To date, analyses of quantum Markov processes and their mixing-time only consider the evolution of a *single* quantum state. However, if the quantum information-processing task involves classical inputs, a classical-quantum (c-q) encoding $E : \mathcal{X} \mapsto \mathcal{D}(\mathcal{H})$ is normally performed before a quantum channel (or circuit). The resulting channel generates a quantum ensemble $W_X \triangleq \{p_X(x), W_x\}_{x\in\mathcal{X}}$, if the classical input X has a distribution p_X. This class of classical-quantum channels and the induced quantum ensembles contain important yet practical applications, e.g., sending classical messages over a quantum channel. Thus how to describe the dynamic evolution of a quantum ensemble W_X is also a fundamentally important question that, as yet, has not been explored. Moreover, a multitude of questions follow. What is the long-term behavior of this ensemble during a Markovian dynamical process? How fast does the ensemble generated converge to its equilibrium? Under what circumstances does the classical-quantum channel lose its capability to communicate information? Finding the answers to those questions will shed light on how those ensembles might be used to help computation or communication.

In this paper, we develop a framework for Markov semigroup theory to characterize the dynamical process of a quantum ensemble W_X, and present preliminary answers to the questions raised above. The proposed semigroups $\{\mathsf{P}_t\}_{t\geq 0}$ acting on the ensemble W_X directly generalize Davies and Lindblad's notion of quantum dynamical semigroups (QDS) Φ_t [1] from a single quantum state to an ensemble. To measure the information content of the ensemble undergoing the proposed Markovian evolution at each time step, we use an entropic quantity—the recently introduced matrix Φ-entropy [2]. We obtain a formula that describes the rate at which the matrix Φ-entropy changes with time. With this formula, we show that the matrix Φ-entropy decays exponentially and its convergence rate is related to the constant in the matrix log-Sobolev inequality (see Theorem 1).

Two special cases of the proposed Markovian dynamical evolution are studied: parallel evolution of each individual state and statistical mixing of quantum states in the ensemble. In the first case, each quantum state is independently evolved with the QDS of depolarizing and phase-damping channels. The equilibrium state in the former is unique; hence, the matrix Φ-entropy will converge to zero for the depolarizing parallel evolution. However, the matrix Φ-entropy can be strictly positive in the latter, since each state can evolve into different equilibrium states. We demonstrate the time evolution of these two channels in the following figure. Next, we consider statistical mixing of quantum states indexed by n-bit strings (a Boolean hypercube). In all these examples, we can explicitly compute the convergence rates.



(a) Depolarizing channel. (b) Phase-damping channel.

*F99942118@ntu.edu.tw
†Min-Hsiu.Hsieh@uts.edu.au
‡marco.tomamichel@sydney.edu.au

Markov semigroups for a quantum ensemble. Consider a time-dependent c-q map $W_t : x \in \mathcal{X} \mapsto W_{t,x} \in \mathcal{D}(\mathcal{H})$ at time t. We denote by $W_{t,X} \triangleq \{p_X(x), W_{t,x}\}$ the quantum ensemble generated by the c-q channel W_t with the input distribution p_X We say that a family of operators $\{\mathsf{P}_t\}_{t\geq 0}$ acting on an ensemble W_x forms a Markov semigroup if they satisfy $\mathsf{P}_s \circ \mathsf{P}_t = \mathsf{P}_{s+t}$. Then we define the Markov semigroup P_t acting on the initial ensemble W_0 by the rule: $W_t : x \mapsto W_{t,x} \triangleq \sum_y \mathsf{T}_t^{x\leftarrow y}(W_{0,y})$, where $\{\mathsf{T}_t^{x\leftarrow y}\}$ be a set of completely positive maps, and $\sum_y \mathsf{T}_t^{x\leftarrow y}$ be a completely positive and trace-preserving (CPTP) unital map. We call the distribution p_X *invariant* to the semigroup $\{\mathsf{P}_t\}_{t\geq 0}$ and the c-q channels $\{W_t\}_{t\geq 0}$ if $\sum_{x\in\mathcal{X}} p_X(x) W_{0,x} = \sum_{x\in\mathcal{X}} p_X(x) W_{t,x}$ for all $t \geq 0$. In other words, the invariant measure p_X ensures that the average state of the ensemble $W_{t,X}$ remained unchanged at each time step.

Matrix Φ-entropy and matrix Φ-Sobolev inequality. We will use the following definition of matrix Φ-entropies to measure the information content of an ensemble W_X:

$$H_\Phi(W_X) \triangleq \operatorname{Tr}\left[\mathbb{E}_X \Phi(W_X) - \Phi(\mathbb{E}_X[W_X])\right], \quad (1)$$

where $\mathbb{E}_X$ denotes taking expectation with respect to the random variable X and the distribution p_X, and Φ is a convex function. The matrix Φ-entropy is introduced in Ref. [2], and has various desirable properties as an entropy measure. Notably, it includes several entropic quantities as a special case. When $\Phi(u) = u^2$, $H_\Phi(W_X)$ equals the variance of the ensemble W_X, $\operatorname{Var}(W_X)$. The Holevo quantity $\chi(W_X)$ can be obtained when $\Phi(u) = u \log u$.

Define the modified energy functional as

$$\mathcal{E}_\Phi(W_X) \triangleq -\operatorname{Tr}\left[\mathbb{E}_X\left[\Phi'(W_X)\,\partial_t \mathsf{P}_t(W_X)\right]\right],$$

where Φ' is the first-order derivative of Φ. We say a matrix Φ-Sobolev inequality exists with a constant $C > 0$ if

$$H_\Phi(W_X) \leq C\mathcal{E}_\Phi(W_X) \quad (2)$$

for all classical-quantum channels W_X.

Exponential decay phenomenon. In the following, we present the main result of the paper: the matrix Φ-entropy admits an exponential decay along the semigroup and the ensemble will converge to its *equilibrium*—the invariant ensemble for P_t. The decaying constant is closely related to the constant in the *matrix Φ-Sobolev inequality.*

Theorem 1 (Main Result)**.**

$$H_\Phi(W_X) \leq C\mathcal{E}_\Phi(W_X) \;\Leftrightarrow H_\Phi(W_{t,X}) \leq \mathrm{e}^{-t/C} H_\Phi(W_{0,X})$$

for all classical-quantum channels W with an invariant distribution p_X.

We remark that Theorem 1 yields a stronger notion of the monotonicity of the Holevo quantity: $\chi(\Phi_t(W_X)) \leq \mathrm{e}^{-t/C}\chi(W_X)$ for every QDS Φ_t. Before concluding the paper, we present two special cases of the semigroup $\{\mathsf{P}_t\}_{t\geq 0}$ and obtain optimal decaying constants for them.

Discussion. In this paper, we study the long-term behaviour of a classical-quantum channel when its input is associated with a probability distribution. To achieve this goal, we also extend the definition of QDS on a single quantum state to that on a classical-quantum map, i.e., a quantum ensemble. This kind of problem is fundamental, and has been studied in both the classical and quantum settings. We summarize those results and contrast with our hybrid classical-quantum scenario in the following table.

Entropy	Classical Ref. [3]	Quantum $\mathbb{L}_p$ relative entropy [4, Def. 3.5]	Classical-Quantum Matrix Φ-entropy Ref. [2]
Log-Sobolev Inequality	Refs. [5, 3]	[4, Def. 3.5]	Eq. (2) & Ref. [8]
Exponential Decay	[3, Corollary 1]	[6, Lemma 21]	Theorem 1

Our main result, Theorem 1, appears similar to Boltzmann's H-Theorem [7], i.e. $H_t \leq \mathrm{e}^{-t/C} H_0$ where $H_t \triangleq \int \mathrm{d}v\, f_t \log f_t$ is the Boltzmann's H-quantity, and f_t is a real-valued function that determines the number of gas particles. Our result can be arguably viewed as the generalization of the above inequality by replacing f_t to a matrix-valued function (or a classical-quantum channel) W. Furthermore, we provide an interesting example that has no classical analogy. In the classical setting, irrelevant to their exact values of the stationary states, Boltzmann's H-quantity will *always* be zero after reaching its equilibrium. On the contrary, the final stationary states of the Markovian evolution of a classical-quantum channel *do* play a crucial role in their long term behaviors. As our two examples of parallel evolution of depolarizing and phase-damping channels show, the existence of a unique fixed stationary quantum state of the depolarizing channel guarantees that the Φ-entropy converges to zero, indicating the ensemble loses its power of being an information carrier. Surprisingly, it is possible that the stationary quantum ensemble resulting from phase-damping channels still contains computational power. It will be interesting to see how useful this kind of quantum phenomena can be in quantum communication and computation.

References

[1] G. Lindblad, Commun. Math. Phys. **48**, 199 (1976).

[2] R. Y. Chen and J. A. Tropp, Electron. J. Probab. **19**,1 (2014).

[3] D. Chafa i, J. Math. Kyoto Univ. **44**, 325 (2004).

[4] R. Olkiewicz and B. Zegarlinski, J. Funct. Anal. **54**, 052202 (2013).

[5] L. Gross Amer.J. Math. **97**, 1061 (1975).

[6] M. J. Kastoryano and K. Temme, J. Math. Phys. **54**, 052202 (2013).

[7] L. Boltzmann, Phys. Today **17**, 76 (1964).

[8] H.-C. Cheng and M.-H. Hsieh arXiv:1506.06801 [quant-ph] (2015).

Strict inequalities for quantum f-divergences and Rényi divergences

Fumio Hiai[1] * Milán Mosonyi[2 3 4] †

[1] *Tohoku University (Emeritus), Hakusan 3-8-16-303, Abiko 270-1154, Japan*
[2] *Institute for Advanced Studies, Technische Universität München, Lichtenbergstraße 2a, 85748 Garching, Germany*
[3] *Zentrum Mathematik, M5, Technische Universität München, Boltzmannstraße 3, 85748 Garching, Germany*
[4] *Mathematical Institute, Budapest University of Technology and Economics, Egry J. u. 1, 1111 Budapest, Hungary*

Abstract.
This submission is based on the paper `https://arxiv.org/abs/1604.03089`.

Keywords: f-divergences, Rényi divergences, relative entropy

1 Petz-type and maximal f-divergences

The concept of classical f-divergences gives a unified framework to construct and study measures of dissimilarity of probability distributions; special cases include the relative entropy and the Rényi divergences. Various quantum versions of this concept, and more narrowly, the concept of Rényi divergences, has been introduced in the literature with applications in quantum information theory. Here we establish various properties of these quantities and relations among them; in particular, we show that in general the different quantum versions of a classical f-divergence strictly differ for non-commuting states under mild technical conditions; that in general measurements strictly decrease the distinguishability of two quantum states unless they commute; and that certain quantum operations strictly decrease certain quantum Rényi divergences of two states unless they can be reversed on the given states.

One very successful construction for quantum f-divergences was developed by Petz [8], defined for every function $f : (0,+\infty) \to \mathbb{R}$ and quantum states ϱ, σ as $S_f^P(\varrho\|\sigma) := \operatorname{Tr} \sigma^{1/2} f\left(L_\varrho R_{\sigma^{-1}}\right) \sigma^{1/2}$, where L_ϱ and $R_{\sigma^{-1}}$ stand for the left- and right multiplications by ϱ and σ^{-1}. The most important examples are the relative entropy $S_\eta^P(\varrho\|\sigma) = \operatorname{Tr} \varrho(\log \varrho - \log \sigma)$, and $S_{f_\alpha}^P(\varrho\|\sigma) = \operatorname{sgn}(\alpha-1) \operatorname{Tr} \varrho^\alpha \sigma^{1-\alpha}$, where η and f_α are as before. The latter quantities give rise to the *standard Rényi divergences* $D_\alpha(\varrho\|\sigma) := \frac{1}{\alpha-1} \log \operatorname{Tr} \varrho^\alpha \sigma^{1-\alpha}$, which, together with the more recently introduced *sandwiched Rényi divergences* $D_\alpha^*(\varrho\|\sigma) := \frac{1}{\alpha-1} \log \operatorname{Tr} \left(\varrho^{1/2} \sigma^{\frac{1-\alpha}{\alpha}} \varrho^{1/2}\right)^\alpha$, are known to quantify the trade-off between the two error probabilities in various hypothesis testing problems; see [7] and references therein.

Other ways to define quantum f-divergences go via optimizing classical f-divergences over pairs of classical probability distributions related to the quantum states. One such approach was introduced and studied in detail by Matsumoto under the name *maximal f-divergence* [6]. For two quantum states ϱ and σ, and a function $f : (0,+\infty) \to \mathbb{R}$, the corresponding maximal f-divergence is defined as $S_f^{\max}(\varrho\|\sigma) := \inf\{S_f(p\|q) : p, q \in \mathcal{B}(\mathcal{K})_+$ are commuting, $\dim \mathcal{K} < +\infty$, and $\Phi(p) = \varrho$, $\Phi(q) = \sigma$ for some CPTP map $\Phi : \mathcal{B}(\mathcal{K}) \to \mathcal{B}(\mathcal{H})\}$. As it was shown in [6], this optimization can be written in an explicit form as $S_f^{\max}(\varrho\|\sigma) = \operatorname{Tr} \sigma^{1/2} f\left(\sigma^{-1/2} \varrho \sigma^{-1/2}\right) \sigma^{1/2}$. By their very definition, the maximal f-divergences are maximal among the monotone (under quantum operations) quantum f-divergences in the sense that for any two states ϱ, σ, any operator convex function $f : (0,+\infty) \to \mathbb{R}$, and any monotone quantum f-divergence S_f^q, we have $S_f^q(\varrho\|\sigma) \le S_f^{\max}(\varrho\|\sigma)$; in particular, this holds for the Petz-type f-divergences. Our first result is that the Petz-type and the maximal f-divergences are strictly different in the following precise sense [3]:

Theorem 1 *Let ϱ, σ be non-commuting states such that $\operatorname{supp} \varrho \subseteq \operatorname{supp} \sigma$. Then*

$$S_f^P(\varrho\|\sigma) < S_f^{\max}(\varrho\|\sigma)$$

for any operator convex function f on $[0,+\infty)$ such that the measure μ_f in the canonical integral representation of f in [4, Theorem 8.1] has a large enough support. In particular, this holds for the most relevant examples $f = \eta$ and $f = f_\alpha$.

2 Measured f-divergences

Measurements can be seen as quantum operations mapping quantum states into classical probability distributions, and hence for any monotone quantum f-divergence S_f^q, one has

$$\begin{aligned} S_f^q(\varrho\|\sigma) &\ge \sup_{\{M_x\}_{x\in\mathcal{X}}} \left\{S_f\left(\{\operatorname{Tr} M_x\varrho\}_{x\in\mathcal{X}} \| \{\operatorname{Tr} M_x\sigma\}_{x\in\mathcal{X}}\right)\right\} \\ &=: S_f^{\mathrm{meas}}(\varrho\|\sigma), \end{aligned} \tag{1}$$

where the supremum is taken over all finite POVMs. It follows from its definition that the measured f-divergence $S_f^{\max}$ is a monotone quantum f-divergence, and by the

*hiai.fumio@gmail.com
†milan.mosonyi@gmail.com

above, it is minimal among all monotone quantum f-divergences, hence it is the dual notion of the above maximal f-divergence. A variant $S_f^{\mathrm{pr}}(\varrho\|\sigma)$ can be defined by requiring the measurements to be projective; it is easy to see that in this case the supremum over measurements becomes a maximum that is attained at a rank-1 projective measurement (von Neumann measurement). Obviously, S_f^{pr} is also a quantum f-divergence, but it is not clear whether it satisfies some of the most natural requirements for a quantum divergence, e.g., invariance under isometric embeddings of its arguments into bigger Hilbert spaces. In fact, we have the following [3]:

Proposition 2 *For any operator convex function f on $(0,+\infty)$, the following are equivalent: (i) S_f^{pr} is monotone non-increasing under CPTP maps; (ii) S_f^{pr} is invariant under isometries; (iii) $S_f^{\mathrm{meas}}(\varrho\|\sigma) = S_f^{\mathrm{pr}}(\varrho\|\sigma)$ for any two states ϱ,σ.*

It is clear that information is lost during the measurement process, and hence the distinguishability of the post-measurement probability distributions cannot be larger than that of the original quantum states, as expressed by the inequality in (1). It is natural to ask whether a measurement can be found that does not decrease the distinguishability. The following result shows that in the case of the Petz-type f-divergences, this is rarely the case unless the two states commute [3]:

Theorem 3 *Let ϱ,σ be states such that $\operatorname{supp}\varrho \subseteq \operatorname{supp}\sigma$. The following are equivalent:*

(i) $S_f^P(\varrho\|\sigma) = S_f\left(\{\operatorname{Tr} M_x\varrho\}_{x\in\mathcal{X}}\|\{\operatorname{Tr} M_x\sigma\}_{x\in\mathcal{X}}\right)$ *for some measurement $\{M_x\}_{x\in\mathcal{X}}$ and some operator convex function f on $[0,+\infty)$ such that $|\operatorname{supp}\mu_f| \geq |\operatorname{spec}(L_\varrho R_{\sigma^{-1}})| + |\mathcal{X}|$.*

(ii) $\varrho\sigma = \sigma\varrho$.

(iii) $S_f^P(\varrho\|\sigma) = S_f^{\mathrm{pr}}(\varrho\|\sigma)$ *for all convex functions $f : (0,+\infty)\to\mathbb{R}$.*

(iv) $S_f^P(\varrho\|\sigma) = S_f^{\mathrm{pr}}(\varrho\|\sigma)$ *for a continuous operator convex function f on $[0,+\infty)$ such that $|\operatorname{supp}\mu_f| \geq |\operatorname{spec}(L_\varrho R_{\sigma^{-1}})| + \dim\operatorname{supp}\sigma$.*

It is an open question whether condition (i) in the above Theorem can be strengthened to $S_f^P(\varrho\|\sigma) = S_f^{\mathrm{meas}}(\varrho\|\sigma)$. This is certainly the case for every f for which $S_f^{\mathrm{meas}} = S_f^{\mathrm{pr}}$, and it was shown very recently in [2] that this holds for the most important examples $f=\eta$ and $f=f_\alpha$, $\alpha\in(0,1)\cup(1,+\infty)$.

3 Monotonicity of α-z Rényi divergences

A two-parameter family of quantum Rényi divergences, called α-z Rényi divergences, was introduced in [1] (see also [5, Section 3.3]), defined as $D_{\alpha,z}(\varrho\|\sigma) := \frac{1}{\alpha-1}\log\operatorname{Tr}\left(\sigma^{\frac{1-\alpha}{2z}}\varrho^{\frac{\alpha}{z}}\sigma^{\frac{1-\alpha}{2z}}\right)^z$ for any $\alpha\in\mathbb{R}\setminus\{1\}$ and $z>0$. This notion encapsulates the previously considered Rényi divergences, as the special case $z=1$, $\alpha>0$ yields the standard Rényi divergences, while $z=\alpha>0$ gives the sandwiched Rényi divergences. Monotonicity of these quantities under CPTP maps has been established for various domains of (α,z) pairs (see [3] and references therein), but a complete characterization of monotonicity is still missing. It is natural to ask when the monotonicity inequality is satisfied with equality. Here we consider the special case where the map Φ is bistochastic, and ϱ or σ is a fixed point of Φ. A particular example of this case is when Φ is a dephasing map, i.e., a (block-)diagonalization in some basis in which one of the states is already (block-)diagonal. Under this assumption, we prove the monotonicity for various (α,z) pairs for which it has not been known before, or actually fails for general CPTP maps. Moreover, we show that in these cases the map does not decrease the α-z Rényi divergence if and only if it is reversible on $\{\varrho,\sigma\}$, i.e., there exists a CPTP map Ψ such that $\Psi(\Phi(\varrho))=\varrho$, $\Psi(\Phi(\sigma))=\sigma$. The exact range of (α,z) pairs for which we prove these is given in [3, Theorem 5.2]. See [3] and references therein also for related results and the history of the reversibility problem.

References

[1] K. M. R. Audenaert and N. Datta. α-z-relative entropies. *J. Math. Phys.*, 56:022202, 2015.

[2] M. Berta, O. Fawzi, and M. Tomamichel. On variational expressions for quantum relative entropies. arXiv:1512.02615, 2015.

[3] F. Hiai and M. Mosonyi. Reversibility of stochastic maps via quantum divergences. arXiv:1604.03089, 2016.

[4] F. Hiai, M. Mosonyi, D. Petz, and C. Bény. Quantum f-divergences and error correction. *Rev. Math. Phys.*, 23:691–747, 2011.

[5] V. Jaksic, Y. Ogata, Y. Pautrat, and C.-A. Pillet. Entropic fluctuations in quantum statistical mechanics. an introduction. In *Quantum Theory from Small to Large Scales, August 2010*, volume 95 of *Lecture Notes of the Les Houches Summer School*. Oxford University Press, 2012.

[6] K. Matsumoto. A new quantum version of f-divergence. arXiv:1311.4722, 2013.

[7] M. Mosonyi and T. Ogawa. Quantum hypothesis testing and the operational interpretation of the quantum Rényi relative entropies. *Comm. Math. Phys.*, 334(3):1617–1648, 2015.

[8] Dénes Petz. Quasi-entropies for finite quantum systems. *Rep. Math. Phys.*, 23:57–65, 1986.

Concavity of Auxiliary Function in Classical-Quantum Channels

Hao-Chung Cheng[1] [2] Min-Hsiu Hsieh[2]

[1] *Graduate Institute Communication Engineering, National Taiwan University, Taiwan (R.O.C.)*
[2] *Centre for Quantum Computation & Intelligent Systems, Faculty of Engineering and Information Technology, University of Technology Sydney, NSW 2007, Australia*

Abstract. The auxiliary function of a classical channel appears in two fundamental quantities, the random coding exponent and the sphere-packing exponent, which yield upper and lower bounds on the error probability of decoding, respectively. A crucial property of the auxiliary function is its concavity, and this property consequently leads to several important results in finite blocklength analysis. In this paper, we prove that the auxiliary function of a classical-quantum channel also enjoys the same concavity property, extending an earlier partial result to its full generality. We also prove that the auxiliary function satisfies the data-processing inequality, among various other important properties. Furthermore, we show that the concavity property of the auxiliary function enables a geometric interpretation of the random coding exponent and the sphere-packing exponent of a classical-quantum channel. The key component in our proof is an important result from the theory of matrix geometric means. Our complete paper can be found in arXiv:1602.03297 [quant-ph].

1 Introduction

Denote by $\mathscr{P}(\mathcal{X})$ the set of probability distributions on a finite set $\mathcal{X} = \{1, 2, \ldots, |\mathcal{X}|\}$. For any fixed $P \in \mathscr{P}(\mathcal{X})$ and $s \geq 0$, the *auxiliary function* $E_0(s, P)$ of a classical communication channel $Q(y|x)$ with the output set $\mathcal{Y} = \{1, 2, \ldots, |\mathcal{Y}|\}$ is defined as

$$E_0(s, P) \triangleq -\log \left[\sum_{y \in \mathcal{Y}} \left(\sum_{x \in \mathcal{X}} P(x) Q(y|x)^{\frac{1}{1+s}} \right)^{1+s} \right]. \quad (1)$$

This function appears in two fundamental quantities in classical information theory: for any $R \geq 0$,

$$E_{\mathrm{r}}(R) \triangleq \max_{0 \leq s \leq 1} \left\{ \max_{P \in \mathscr{P}(\mathcal{X})} E_0(s, P) - sR \right\}, \quad (2)$$

$$E_{\mathrm{sp}}(R) \triangleq \sup_{s \geq 0} \left\{ \max_{P \in \mathscr{P}(\mathcal{X})} E_0(s, P) - sR \right\}, \quad (3)$$

where $E_{\mathrm{r}}(R)$ is called the *random coding exponent* and $E_{\mathrm{sp}}(R)$ is called the *sphere-packing exponent* of the classical channel Q. These two quantities are critical since, for any block length n and any rate $0 \leq R \leq C$, where C denotes the capacity of the channel W, the error probability $P_e(n, R)$, minimized over all possible coding strategies, satisfies: [1]–[3]

$$2^{-nE_{\mathrm{sp}}(R)} \lesssim P_e(n, R) \lesssim 2^{-nE_{\mathrm{r}}(R)}. \quad (4)$$

Consequently, properties of the auxiliary function $E_0(s, P)$ reveal important functional behaviour of the two exponents, and lead to a deeper understanding of the error probability of a given classical channel Q. It is well-known (and easy to show) [3]: (1) $E_0(s, P) \geq 0$; (2) $\frac{\partial E_0(s,P)}{\partial s} > 0$; (3) $\frac{\partial^2 E_0(s,P)}{\partial s^2} \leq 0$ for all $s \geq 0$. It turns out that $E_0(s, P)$ is concave in $s \geq 0$. In addition to other important contributions in finite block length analysis, this fact also provides an alternative proof to Shannon's noiseless channel coding theorem [4].

In recent years, much attention has been paid to understanding the reliable transmission of classical messages through a quantum channel. In this scenario, it suffices to consider a *classical-quantum channel*, which is a mapping $W : x \in \mathcal{X} \mapsto W_x \in \mathcal{S}(\mathcal{H})$ from the finite set $\mathcal{X}$ to $\mathcal{S}(\mathcal{H})$, the set of density operators (positive semi-definite operators with unit trace) on a fixed Hilbert space $\mathcal{H}$. Given a classical-quantum channel W and a distribution P on the input $\mathcal{X}$, we can similarly define the *auxiliary function* $E_0(s, P, W)$ [5], [6]: $\forall s \geq 0$,

$$E_0(s, P, W) \triangleq -\log \mathrm{Tr} \left[\left(\sum_{x \in \mathcal{X}} P(x) \cdot W_x^{\frac{1}{1+s}} \right)^{1+s} \right]. \quad (5)$$

This quantity is a quantum generalization of Eq. (1), and recovers Eq. (1) when all $\{W_x\}_{x \in \mathcal{X}}$ commute. When no confusion is possible, we ignore the argument W in $E_0(s, P, W)$.

The auxiliary function $E_0(s, P)$ in Eq. (5) also appears in the random coding exponent $E_{\mathrm{r}}(R)$ and the sphere-packing exponent $E_{\mathrm{sp}}(R)$ of a classical-quantum channel W, which can be similarly defined as that in Eqs. (2) and (3), respectively. However, relations between these two exponents and the error probability of the underlining classical-quantum channel W are much harder to obtain. The random coding exponent $E_{\mathrm{r}}(R)$ is shown to be an upper bound to the error probability of a classical-quantum channel W when every W_x is a pure state in Ref. [5], and it is conjectured to hold for general quantum states. Furthermore, the sphere-packing bound that lower bounds the error probability of W was recently proved in Ref. [7]. These results are highly nontrivial due to the non-commutative nature of the density operators involved in their definitions. Many important questions in quantum information theory are still left open. Notably, it is still unknown whether the auxiliary function $E_0(s, P)$ in Eq. (5) is concave for all $s \geq 0$. This might be one reason that the error probability of any finite block length n is less understood in the quantum regime. Note

that $E_0(s,P)$ has been shown to be concave in $0 \le s \le 1$ in Ref. [8]. Its proof relies on an *ad-hoc* operator inequality in order to show that the second-order derivative of $E_0(s,P)$ is non-positive for $s \in [0,1]$. However, this method seems impossible to work for all $s \ge 0$.

In this paper, we prove that $E_0(s,P)$ of a classical-quantum channel W is concave for all $s \ge 0$. Our proof culminates the latest development of operator algebra; in particular, the beautiful theory of a general geometric mean of operators [9].

2 Technical Tools: Geometric Means

For two positive definte matrices A, B, define the "s-weighted geometric mean" of A and B as

$$A\#_s B \triangleq A^{1/2}\left(A^{-1/2}BA^{-1/2}\right)^s A^{1/2}. \tag{6}$$

for all $s \in [0,1]$. The geometric mean is our key ingredient to our main result (Theorem 2), which enjoys the following properties.

Proposition 1 (Properties of Geometric Means [9])**.** *The map $(A,B) \mapsto A\#_s B$ is jointly concave, $\forall 0 \le s \le 1$.*

3 Main Result

Our main result is to prove the concavity of the auxiliary function:

Theorem 2. *Given a classical-quantum channel $W \in \mathscr{W}(\mathcal{X})$ and a distribution $P \in \mathscr{P}(\mathcal{X})$, the auxiliary function $E_0(s,P)$ is concave in s for all $s \ge 0$.*

4 Properties of the Auxiliary Function

This section presents important properties of the auxiliary function.

Proposition 3. *The auxiliary function $E_0(s,P,W)$ has the following properties.*

(a) Monotonicity: $E_0(s,P,W) \le E_0(t,P,W)$ *for all* $0 \le s \le t$.

(b) Non-negativity: $E_0(s,P,W) \ge 0$ *for all* $s \ge 0$ *with* $E_0(0,P,W) = 0$.

(c) Relation with mutual information: $\partial E_0(s,P,W)/\partial s|_{s=0} = I(P,W)$.

(d) Concavity in s: $\frac{\partial^2 E_0(s,P,W)}{\partial s^2} \le 0$ *for all* $s \ge 0$.

(e) Convexity in W: *The map* $W \mapsto E_0(s,P,W)$ *is convex.*

(f) Convexity in P: *The map* $P \mapsto \exp(-E_0(s,P,W))$ *is convex.*

(g) Tensor invariance: $E_0(s,P,W\otimes\varrho) = E_0(s,P,W)$, *for some subsystem* $\varrho \in \mathcal{S}(\mathcal{H})$.

(h) Unitary invariance: $E_0(s,P,UWU^\dagger) = E_0(s,P,W)$, *where* $UWU^\dagger$ *is the unitary conjugation of* W.

(i) Data-processing inequality: $E_0(s,P,\Phi\circ W) \le E_0(s,P,W)$ *for any completely-positive and trace-preserving map* Φ.

(j) Conditions for maximization over P: *The input distribution P attains $E_0(s,P,W)$, if and only if*

$$\mathrm{Tr}\left[W_x^{1/(1+s)}\left(\sum_{x\in\mathcal{X}} P(x)W_x^{1/(1+s)}\right)^s\right] \ge \mathrm{Tr}\left[\left(\sum_{x\in\mathcal{X}} P(x)W_x^{1/(1+s)}\right)^{1+s}\right], \quad \forall x \in \mathcal{X}.$$

4.1 Relations to Random Coding Exponent and Sphere-Packing Exponent

The concavity property of the auxiliary function allows us to better characterize the random coding exponent and the sphere packing exponent:

Proposition 4. *Both the random coding exponent $E_r(R)$ and the sphere-packing exponent $E_{\mathrm{sp}}(R)$ are decreasing and strictly convex in R.*

5 Conclusion

In this paper, we proved an open question that was originally raised in Ref. [6]. A partial result to this question was obtained in Ref. [8]; however, we can extend the concavity of the auxiliary function $E_0(s,P)$ for all $s \ge 0$. Consequently, the definition of the auxiliary function Eq. (5) of a classical-quantum channel exactly recovers its classical counterpart [3], a quantity that plays a crucial role in classical information theory. We hope that this concave property will also allow us to better characterize the error probability of a classical-quantum channel in the finite regime.

References

[1] R. Gallager, *IEEE Inform. Theory* **11**(1): 3–18, (1965).

[2] C. Shannon, R. Gallager and E. Berlekamp, *Inform. and Control* **10**(1): 65–103, (1967).

[3] R. Gallager, *Information Theory and Reliable Communication* (1968).

[4] C. Shannon, *Bell. J.* **27**:379–426, (1948).

[5] M. Burnashev and A. Holevo, *IEEE Inform. Theory* **34**(2): 97–107, (1998).

[6] A. Holevo, *IEEE Inform. Theory* **46**(11): 2256–2261, (2000).

[7] M. Dalai, *IEEE Inform. Theory* **59**(12): 8027–8056, (2013).

[8] J. Fujii, R. Nakamoto and K. Yanagi, *IEEE Inform. Theory* **52**(7): 3310–3313, (2016).

[9] F. Kubo and T. Ando, *Math. Annal.* **246**(3): 205–224, (1980).