Classical-quantum channels with causal and non-causal channel state information at the sender

Holger Boche, Ning Cai, Janis Nötzel

ISIT 2016
Barcelona
14. Juli 2016

More information at

arXiv:1506.06479

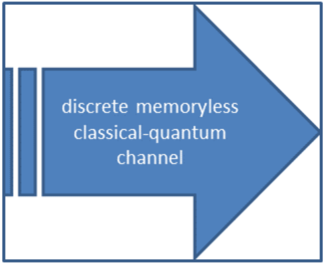
Previous work on the topic

Gel'fand and Pinsker [GP80]
Dupuis [Dup09]

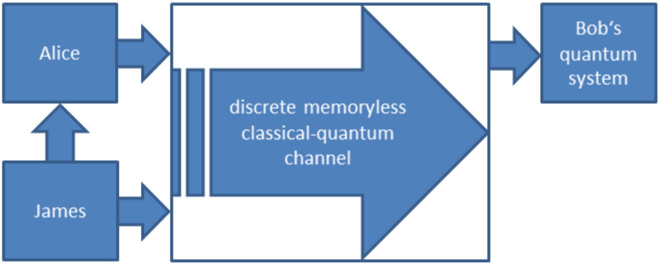
Outline

1. Model
2. Basics
3. Definitions
4. Results
5. Ingredients
6. Conclusion

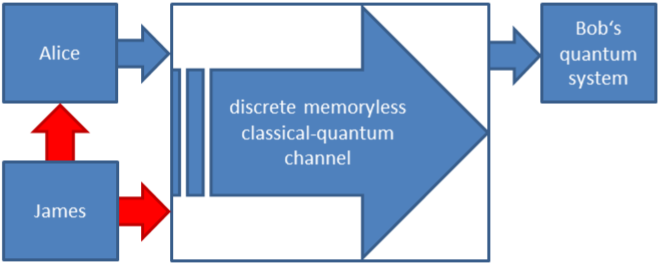
❶ Model



❶ Model


Alice
James
discrete memoryless
classical-quantum
channel
Bob's
quantum
system

❶ Model



Needs careful distinction between causal and non-causal codes, that is not simply displayed in this "one-shot" picture.

❶ Model / non-causal codes

Time	Alice	Bob	James
-5	Agree on code $\mathcal{K}_n$		
-4			Receive code $\mathcal{K}_n$
-3			Choose $s^n \sim p^{\otimes n}$
-2	Receive s^n		
-1	Pick $m \in [M_n]$		
0	Encode $\sim E(m, s^n)$		
1	send x_1		
…	…	…	…
n	send x_n		
n+1		Decode	

❶ Model / causal codes

Time	Alice	Bob	James
-3	Agree on code $\mathcal{K}_n$		
-2			Receive code $\mathcal{K}_n$
-1			Choose $s^n \sim p^{\otimes n}$
0	Pick $m \in [M_n]$		
1	Receive s_1		
1	Send $x_1 \sim E_1(m, s_1)$		
2	Receive s_2		
2	Send $x_2 \sim E_2(m, s^2)$		
...	...	...	...
n+1		Decode	

- The quantum systems $\mathcal{K}$ under consideration are modeled on finite dimensional Hilbert spaces labelled by the same letter $\mathcal{K}$.
- A classical-quantum (cq) channel takes inputs from a finite set $\mathbf{Y}$, generating outputs in $\mathcal{K}$. The set of all such channels is $CQ(\mathbf{Y}, \mathcal{K})$.
- For us, $\mathbf{Y} = \mathbf{S} \times \mathbf{X}$, where Alice controls $\mathbf{X}$ and James controls $\mathbf{S}$.
- Inputs made by James (channel states) are revealed to Alice but not to Bob.
- James chooses inputs randomly according to $p \in \mathfrak{P}(\mathbf{X})$.
- The channel is memoryless over n channel uses, the jammer's choice i.i.d. according to p.
- Thus, the system is completely described by the pair $(W_{\mathbf{S}\times\mathbf{X}\to\mathcal{K}}, p)$.
- We distinguish two cases: First when Alice has causal channel knowledge, second when she has non-causal channel state knowledge.

- Forget about James (for the moment).

- Forget about James (for the moment).
- Alice has messages $[M] = \{1, \ldots, M\}$. She wants to send them to Bob.
- Alice uses a stochastic encoding E, which assigns to her message m the code word x with probability $e(x|m)$.
- She puts x into $W \in CQ(\mathbf{X}, \mathcal{K})$, and Bob receives ρ_x.
- Bob tries to guess the message - he measures the output system with a POVM $\mathbf{D} = (D_1, \ldots, D_m)$.
- Probability of (perhaps wrongly) guessing m when m' was sent over channel W:

$$\sum_{x \in \mathbf{X}} e(x|m') \mathrm{tr}\{ D_m \cdot \rho_x \}.$$

- Measure of successful transmission:

$$\frac{1}{M} \sum_m \sum_x e(x|m) \mathrm{tr}\{ D_m \cdot \rho_x \} \in [0, 1].$$

❸ Definitions

- Non-causal code $\mathcal{K}_n$: $M_n \in \mathbb{N}$, $E : [M_n] \times \mathbf{S}^n \to \mathfrak{P}(\mathbf{X}^n)$ and a decoding POVM $\mathbf{D}$ on $\mathcal{K}^{\otimes n}$. Its average error is

$$\mathrm{err}(\mathcal{K}_n) := 1 - \sum_{m=1}^{M_n} \sum_{s^n, x^n} \frac{p^{\otimes n}(s^n)}{M_n} e(x^n|m, s^n) \mathrm{tr}\{\rho_{s^n, x^n} D_m\}.$$

- Causal code: for $t \in [n]$ the distributions $e_t(\cdot|m, s^n) \in \mathfrak{P}(\mathbf{X}^t)$, $e_t(x^t|m, s^n) := \sum_{(x_{t+1},\dots,x_n)} e(x^n|m, s^n)$, depend only on s^t.
- A number $R \geq 0$ is a (non-) causally achievable rate if there exists a sequence $(\mathcal{K}_n)_{n\in\mathbb{N}}$ of (non-) causal codes such that

$$\lim_{n\to\infty} \mathrm{err}(\mathcal{K}_n) = 1, \qquad \liminf_{n\to\infty} \frac{1}{n} \log(M_n) \geq R.$$

- The non-causal capacity C of $(W_{\mathbf{S}\times\mathbf{X}\to\mathcal{K}}, p)$ is the supremum over all rates that are non-causally achievable for $(W_{\mathbf{S}\times\mathbf{X}\to\mathcal{K}}, p)$.
- The causal capacity C_c of $(W_{\mathbf{S}\times\mathbf{X}\to\mathcal{K}}, p)$ is the supremum over all rates that are causally achievable for $(W_{\mathbf{S}\times\mathbf{X}\to\mathcal{K}}, p)$.

- Any map $E : \mathbf{U} \to \mathfrak{P}(\mathbf{X})$ defines a new channel $\tilde{W}_{\mathbf{U}\times\mathbf{S}\to\mathcal{K}} := W_{\mathbf{S}\times\mathbf{X}\to\mathcal{K}} \circ E$ via $\tilde{\rho}_{s,u} := \sum_{x\in\mathbf{X}} e(x|u)\rho_{s,x}$.

Theorem

Let $W_{\mathbf{S}\times\mathbf{X}\to\mathcal{K}} \in CQ(\mathbf{S}\times\mathbf{X},\mathcal{K})$, $p \in \mathfrak{P}(\mathbf{S})$. Then

$$C_c(W_{\mathbf{S}\times\mathbf{X}\to\mathcal{K}}, p) = \max_{q\in\mathfrak{P}(\mathbf{U})} \max_{V\in T} \chi(q, W_{\mathbf{S}\times\mathbf{X}\to\mathcal{K}} \circ V)$$

where T is the set of classical channels with conditional probability distributions of the form

$$v(s,x|u) = \tilde{v}(x|s,u)p(s) \ \ \forall\ (s,u,x) \ \in \mathbf{S}\times\mathbf{U}\times\mathbf{X}.$$

Cardinality bounds apply.

Theorem

It holds $C(W_{\mathbf{S}\times\mathbf{X}\to\mathcal{K}}, p) = \lim_{n\to\infty} \frac{1}{n} C_c(W^{\otimes n}_{\mathbf{S}\times\mathbf{X}\to\mathcal{K}}, p^{\otimes n})$.

Further, for all $n \in \mathbb{N}$,

$$C(W_{\mathbf{S}\times\mathbf{X}\to\mathcal{K}}, p) \geq \frac{1}{n} \max_{q\in A_n} \left(\chi(q_{\mathbf{U}_n}, W_{\mathbf{U}_n\to\mathcal{K}^{\otimes n}}) - I(U_n; S^n)\right).$$

Here we set $A_n := \{q_{\mathbf{S}^n\mathbf{U}_n\mathbf{X}^n} \in \mathfrak{P}(\mathbf{S}^n, \mathbf{U}, \mathbf{X}^n) : q_{\mathbf{S}^n} = p^{\otimes n}\}$ *and to every* $q \in A_n$ *we define* $W_{\mathbf{U}_n\to\mathcal{K}^{\otimes n}}$ *via*

$$W_{\mathbf{U}_n\to\mathcal{K}^{\otimes n}}(u) := \sum_{s^n, x^n} q(s^n, x^n|u) W^{\otimes n}_{\mathbf{S}\times\mathbf{X}\to\mathcal{K}}(s^n, x^n).$$

It may be assumed that $|\mathbf{U}_n| \leq (|\mathbf{S}| \cdot 2 \cdot |\mathbf{X}|)^n$. *In addition,*

$$C(W_{\mathbf{S}\times\mathbf{X}\to\mathcal{K}}, p) = \lim_{n\to\infty} \frac{1}{n} \max_{q\in A_n} \left(\chi(p_{\mathbf{U}_n}, W_{\mathbf{U}_n\to\mathcal{K}^{\otimes n}}) - I(U_n; S^n)\right).$$

❺ Ingredients / Direct Part of Proof

- Use sequential decoding [Aar06,Sen11,Wil15,Gao15]
- "Typical" projections as defined in [Nöt14], exploiting some representation theory
- Codewords are sampled i.i.d. according to flat distribution on set of specified type
- Given a particular choice s^n of James, the encoder sends sequences that are jointly typical s^n

⑥ Conclusions / related work

- Surprisingly, we were not able to get a single-letter formula for non-causal encoding.
- This is less surprising when taking into account that the usual $c \to qq$ wiretap channel [Dev05,CWY04] has no such capacity formula as well.
- Thus we found a new instance of a coding theorem where new ideas seem necessary to gain a deeper understanding.
- Where do things go wrong? $\to$ next slide!

⑥ Conclusions / painpoint

- Proof of converse in classical setting [GP80] uses a telescoping argument similar to the Csiszar-sum identity (find different versions of such identities in [Kra11], where the relation to the classical Gel'fand Pinsker problem is explained)
- Standard arguments yield (both for causal and non-causal encoding)

$$\log(M_n) \leq \sum_{i=1}^{n} I(\mathfrak{M}_n, Q^{i-1}; Q_i) + n \cdot \epsilon_n \cdot |\mathbf{X}|,$$

where the overall state of the quantum system is

$$\sigma := \sum_{m,\hat{m}} \sum_{s^n,x^n} \frac{p^{\otimes n}(s^n)}{M_n} \cdot \psi_m \otimes \psi_{s^n} \\ \otimes e(x^n|m,s^n)\psi_{x^n} \otimes \rho_{s^n,x^n} \otimes \mathrm{tr}\{D_{\hat{m}}\rho_{s^n,x^n}\}\psi_{\hat{m}}$$

and I the quantum mutual information.

THANK YOU.

References

[GP80] S. I. Gel'fand and M. S. Pinsker, "Coding for channels with random parameters", Probl. Control and Inform. Theory, Vol. 9, No. 1, 19-31 (1980)

[Dup09] "The capacity of quantum channels with side information at the transmitter ", Inf. Theory, 2009. ISIT 2009. IEEE Intern. Symposium on, 948-952 (2009)

[Aar06] S. Aaronson, Comp. Compl., 2006. CCC 2006. 21st Ann. IEEE Conf. 13-273 (2006)

[Sen11] P. Sen, "Achieving the Han–Kobayashi inner bound for the quantum interference channel by sequential decoding", preprint, http://arxiv.org/abs/1109.0802 (2011)

[Wil15] M.M. Wilde, "Sequential decoding of a general classical-quantum channel", Proc. R. Soc. A 469: 20130259 (2015)

[Gao15] J. Gao, "Quantum union bounds for sequential projective measurements", to appear in Phys. Rev. A

[Nöt14] J. Nötzel, "Hypothesis testing on invariant subspaces of the symmetric group: part I. Quantum Sanov's theorem and arbitrarily varying sources", J. Phys. A: Math. Theor. 47 235303 (2014)

[Dev05] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel", IEEE Trans. Inf. Theory, 51(1):44–55 (2005)

[CWY04] N. Cai, A. Winter, R.W. Yeung, "Quantum privacy and quantum wiretap channels", Probl. Inf. Transm. Vol. 40, No. 4, 318-336 (2004)

[Kra11] G. Kramer, "Teaching IT: An Identity for the Gelfand-Pinsker Converse", IEEE Inf. Theory Soc. Newsletter (2011)