Game-theoretic characterization of antidegradable channels

Francesco Buscemi, Nilanjana Datta, Sergii Strelchuk *

Full version of paper: arXiv:1404.0277

Deciding whether a given quantum channel has a positive capacity is a non-trivial problem – there does not exist a unique criterion to determine whether the quantum capacity of a given channel is zero. Classical channels with zero capacity are uninteresting in the information-theoretic sense. In contrast, quantum channels with zero capacity exhibit intriguing behavior as shown by the superactivation phenomenon [8]: there exist examples of pairs of channels with zero quantum capacity, which, when used in tandem, allow transmission of quantum information. One particular class of zero-capacity channels consists of *antidegradable channels*. For such a channel, a post-processing of its environment can simulate the output of the channel. The no-cloning theorem [1] ensures that such channels have zero quantum capacity. The simplest example of the latter is a 50% erasure channel which with equal probability either transmits the input state perfectly or replaces it with an erasure flag. However, there are other non-trivial examples of channels with zero quantum capacity, e.g. the positive partial transpose (PPT) channels [2]. In addition, antidegradable channels also have zero private capacity (unlike PPT channels), but whether they are the only non-trivial quantum channels with this property is an open question. Therefore, the knowledge that a given channel has zero quantum and private capacity is not sufficient to conclude that it is antidegradable. This leads us to the following question:

(Q): Is there a setting in which one can obtain a complete operational characterization of antidegradable channels?

We answer this question in the affirmative by constructing a game-theoretic framework which involves the noisy quantum channel $\mathcal{N}$ (which we wish to characterize), a quantum public side channel $\mathcal{S}$, and three parties: Alice (the sender), Bob (the receiver) and Eve (the eavesdropper). Alice sends classical information to Bob through $\mathcal{N}$, whose environment is accessible to Eve. Alice also sends information through $\mathcal{S}$, which is accessible to both Bob and Eve.

The game is constructed as follows.

1. Alice chooses a letter x at random from a given finite alphabet $\mathscr{X}$, and encodes it in a bipartite state, say $\rho^x_{AA_0}$.
2. The A part of the input is sent through $\mathcal{N}$, while the A_0 part is transmitted via $\mathcal{S}$.
3. Bob then obtains the output of $\mathcal{N}$ while Eve receives the information that is transmitted to the channel's environment. In addition, they both receive the output of $\mathcal{S}$.
4. The task now, for both Bob and Eve, is to guess which letter x Alice chose. Since Bob and Eve are competing, they both adopt the optimal guessing strategy they have available. Correspondingly, the reliabilities of their guesses is measured by the optimal guessing probabilities of the ensembles of states they receive.
5. Bob wins the game whenever his guessing probability is *strictly higher* than that of Eve (i.e. in the case of a draw, Eve wins).

The situation is depicted in the Figure below. To introduce the game formally, we start from the following definitions:

*Francesco Buscemi is with Graduate School of Information Science, Nagoya University. Nilajana Datta is with Statistical Laboratory, University of Cambridge. Sergii Strelchuk is with Department of Applied Mathematics and Theoretical Physics, University of Cambridge.

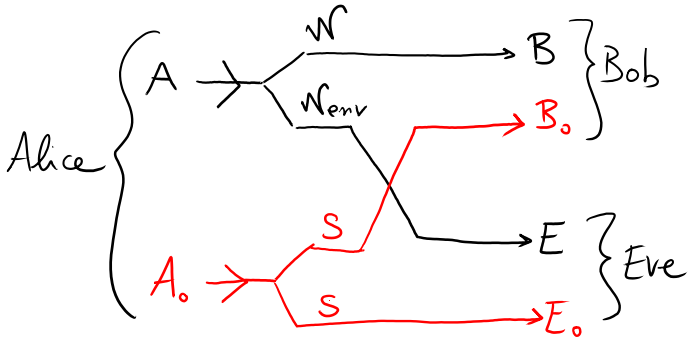

Figure 1: Structure of the guessing game: Alice communicates with Bob using the quantum channel $\mathcal{N}$ (i.e. the one which we want to characterize) and a quantum channel $\mathcal{S}$, which is public, in the sense that it conveys the same output to Bob and Eve. A natural example of such a public channel is a symmetric channel [16, 17, 18]. Bob plays the guessing game against Eve, who has access to the environment of $\mathcal{N}$ (labelled by $\mathcal{N}_{\rm env}$) and $\mathcal{S}$.

Definition 1. *A* (finite) ensemble of quantum states $\mathfrak{m}$ *is defined as a triple* $(\mathcal{H}, \mathscr{X}, \mathcal{E})$*, where* $\mathcal{H}$ *is a finite-dimensional input Hilbert space,* $\mathscr{X} = \{x\}$ *is a finite indexing alphabet, and* $\mathcal{E} = \{p_x, \rho^x\}_{x\in\mathscr{X}}$ *is a collection of quantum states* $\rho^x \in \mathbf{S}(\mathcal{H})$ *and probabilities* p_x*.*

Consider now a quantum channel $\mathcal{N}^{A\to B} : \mathcal{H}_A \to \mathcal{H}_B$ and an ensemble $\mathfrak{m} = (\mathcal{H}_A, \mathscr{X}, \mathcal{E})$. We can then imagine the situation in which a sender (say, Alice) chooses a letter $x \in \mathscr{X}$ at random according to the probability distribution p_x, prepares a quantum system in the corresponding state ρ^x_A, and sends this through $\mathcal{N}$ to a receiver (say, Bob), who has to guess the input letter chosen by Alice. This setup can be formally described as follows:

Definition 2 (Dynamical guessing games)**.** *Let* $\mathcal{N}^{A\to B}$ *be a quantum channel,* $(\mathcal{H}_A, \mathscr{X}, \mathcal{E})$ *an ensemble. The corresponding guessing game is defined as the task of correctly guessing letter* x *upon receiving* $\mathcal{N}(\rho^x_A)$*. The optimal probability of winning the game is given by*

$$p^*(\mathcal{N}, \mathfrak{m}) := \max_{\mathbb{P}_B} \sum_{x\in\mathscr{X}} p_x \operatorname{Tr}[P^x_B\, \mathcal{N}(\rho^x_A)]. \tag{1}$$

Equation (1) above measures 'how good' a given channel $\mathcal{N}$ is for communicating the information about $\mathscr{X}$ encoded in $\mathfrak{m}$. Accordingly, given another channel $\mathcal{M}$, with same input space but generally different output space, one can say that '$\mathcal{N}$ is not worse than $\mathcal{M}$ with respect to $\mathfrak{m}$' if $p^*(\mathcal{N}, \mathfrak{m}) \geqslant p^*(\mathcal{M}, \mathfrak{m})$. By extending this definition to every possible finite ensemble, we obtain the following partial ordering relation between quantum channels:

Definition 3. *Given two quantum channels with the same input space* $\mathcal{N}^{A\to B}_\alpha$ *and* $\mathcal{N}^{A\to B'}_\beta$*, we say that '*$\mathcal{N}^{A\to B}_\alpha$ *is more informative than* $\mathcal{N}^{A\to B'}_\beta$*,' and denote it as* $\mathcal{N}^{A\to B}_\alpha \supseteq \mathcal{N}^{A\to B'}_\beta$*, whenever* $p^*(\mathcal{N}^{A\to B}_\alpha, \mathfrak{m}) \geqslant p^*(\mathcal{N}^{A\to B'}_\beta, \mathfrak{m})$*, for all finite ensembles* $\mathfrak{m}$ *on* $\mathcal{H}_A$*.*

Clearly, guessing games can be also played with more than one channel arranged 'in parallel,' as follows. Consider for example two quantum channels $\mathcal{N}^{A\to B}$ and $\mathcal{M}^{A_0\to B_0}$ and an ensemble defined on the tensor product space $\mathcal{H}_A \otimes \mathcal{H}_{A_0}$, i.e. $\mathfrak{n} = (\mathcal{H}_A \otimes \mathcal{H}_{A_0}, \mathscr{X}, \mathcal{E})$. Then, in analogy with (1), we have

$$p^*(\mathcal{N}^{A\to B} \otimes \mathcal{M}^{A_0\to B_0}, \mathfrak{n}) = \max_{\mathbb{P}_{BB_0}} \sum_{x\in\mathscr{X}} p_x \operatorname{Tr}[P^x_{BB_0}\, (\mathcal{N}^{A\to B} \otimes \mathcal{M}^{A_0\to B_0})(\rho^x_{AA_0})]. \tag{2}$$

It is important to stress that, as the input states $\rho^x_{AA_0}$ can be entangled, so the elements $P^x_{BB_0}$ of the decoding POVM are allowed to act globally on the output. By means of parallelized guessing games, a stronger partial ordering relation can be introduced as follows:

Definition 4 (Strong information ordering)**.** *Given two quantum channels with the same input space* $\mathcal{N}^{A\to B}_\alpha$ *and* $\mathcal{N}^{A\to B'}_\beta$*, we say that '*$\mathcal{N}^{A\to B}_\alpha$ *is strongly more informative than* $\mathcal{N}^{A\to B'}_\beta$*,' and denote it as*

$$\mathcal{N}^{A\to B}_\alpha \supseteq_{\rm s} \mathcal{N}^{A\to B'}_\beta,$$

whenever $\mathcal{N}^{A\to B}_\alpha \otimes \mathcal{M}^{A_0\to B_0} \supseteq \mathcal{N}^{A\to B'}_\beta \otimes \mathcal{M}^{A_0\to B_0}$*, for all quantum side channels* $\mathcal{M}^{A_0\to B_0}$*.*

In the above definition, we allow the comparison between $\mathcal{N}_\alpha$ and $\mathcal{N}_\beta$ to be made in parallel with any possible quantum side channel $\mathcal{M}^{A_0\to B_0}$ considered as an auxiliary communication resource. It is often interesting, however, to constrain the side channel to belong to some restricted class of channels, typically with reduced communication capability. As a trivial example, Definition 3 can be considered as a special case of Definition 4, in which side channels are restricted to those which map all input states to the same output state. We will be interested in the case in which the quantum side channel is a symmetric channel $\mathcal{S}$, ie. such that there exists another channel $\mathcal{D}$ such that $\mathcal{S} = \mathcal{D} \circ \mathcal{N}_{\text{env}}$, where $\mathcal{N}_{\text{env}}$ is a complementary channel to $\mathcal{S}$.

To state our main result (Theorem 1) which leads to the characterization of antidegradable channels, we first introduce the notion of *extension* of a quantum channel: for any pair of quantum channels $(\mathcal{N}_\alpha, \mathcal{N}_\beta)$ we say that $\mathcal{N}_\alpha$ is an *extension* of $\mathcal{N}_\beta$ if $\mathcal{N}_\beta = \mathcal{D} \circ \mathcal{N}_\alpha$ for some quantum channel $\mathcal{D}$. Then our result can be stated as follows: the channel is anti-degradable for any given input ensemble of states, the guessing probability of the output ensemble of a channel is lower than that of its extension. We establish the above result by first proving its analogue for statistical comparison of bipartite states and then using Choi isomorphism to translate it to quantum channels.

Consider the case in which $\mathcal{N}_\beta$ is the quantum channel $\mathcal{N}$ employed in the guessing game, and $\mathcal{N}_\alpha$ is the channel $\mathcal{N}_{\text{env}}$ which is complementary to it. For this choice, our result (Theorem 1) implies that $\mathcal{N}$ is antidegradable *if and only if* Eve always wins, regardless of the choice of Alice's encoding strategy. In other words, *for any* channel which is not antidegradable, there exists (at least) one encoding strategy which Alice can choose to make Bob win the guessing game.

Main technical result and implications

Theorem 1. *Let $\mathcal{N}_\alpha^{A\to B}$ and $\mathcal{N}_\beta^{A\to B'}$ be two quantum channels. Then, the following are equivalent:*

1. *There exists a third quantum channel $\mathcal{D}^{B\to B'}$ such that $\mathcal{N}_\beta^{A\to B'} = \mathcal{D}^{B\to B'} \circ \mathcal{N}_\alpha^{A\to B}$;*
2. *$\mathcal{N}_\alpha^{A\to B} \supseteq_{\text{s}} \mathcal{N}_\beta^{A\to B'}$;*

An interesting interpretation of Theorem 1 is obtained when $\mathcal{N}_\beta$ and $\mathcal{N}_\alpha$ are taken to be the channel $\mathcal{N}$ (which we wish to characterize) and its corresponding complementary channel $\mathcal{N}_{\text{env}}$, respectively. In this situation, consider the guessing game described above where, at each turn of the game (corresponding to each use of the channel), Bob and Eve are asked to guess the input chosen by Alice. In this case, it is natural to require the side-channel $\mathcal{S}$ to be symmetric, so that it serves as a public channel [16, 17, 18], since it conveys the same information to Bob and Eve.

Theorem 1 then implies the following corollary which provides a complete characterization of antidegradable channels in our game-theoretic framework:

Corollary 1. *A quantum channel is not antidegradable if and only if there exists an encoding strategy for Alice which results in Bob winning the game.*

To summarize, we introduced a game-theoretic framework which allowed us to derive a necessary and sufficient condition for a quantum channel to be antidegradable. We showed that for any quantum channel which is not antidegradable, there exists an encoding strategy for which such a channel provides a strict advantage for the two players over the adversary in the guessing game that we defined. The key ingredients in the proof of this result are the tools of statistical comparison of bipartite quantum states, and the Choi isomorphism.

References

[1] W. K. Wootters and W. H. Zurek, *A single quantum cannot be cloned*, , Published online: 28 October 1982; | doi:10.1038/299802a0, 299 (1982), pp. 802–803.

[2] P. Horodecki, M. Horodecki, and R. Horodecki, *Binding entanglement channels*, quant-ph/9904092, (1999). J.Mod.Opt. 47 (2000) 347-354.

[3] K. Li, A. Winter, X. Zou, and G. Guo, *Private capacity of quantum channels is not additive*, Physical Review Letters, 103 (2009), p. 120501.

[4] G. Smith and J. A. Smolin, *Extensive nonadditivity of privacy*, Physical Review Letters, 103 (2009), p. 120503.

[5] G. Smith and J. A. Smolin, *Detecting incapacity of a quantum channel*, Physical Review Letters, 108 (2012), p. 230507.

[6] F. G. S. L. Brandão, J. Oppenheim, and S. Strelchuk, *When does noise increase the quantum capacity?*, Phys. Rev. Lett., 108 (2012), p. 040501.

[7] G. Smith, J. A. Smolin, and J. Yard, *Quantum communication with gaussian channels of zero quantum capacity*, Nature Photonics, 5 (2011), pp. 624–627.

[8] G. Smith and J. Yard, *Quantum communication with zero-capacity channels*, Science, 321 (2008), pp. 1812–1815.

[9] W. F. Stinespring, *Positive functions on C^*-algebras*, Proc. Amer. Math. Soc., 6 (1955), pp. 211–216.

[10] E Shmaya, *Comparison of information structures and completely positive maps*. J. Phys. A: Math. and Gen. **38**, 9717-9727 (2005).

[11] A Chefles, *The Quantum Blackwell Theorem and Minimum Error State Discrimination*. ArXiv:0907.0866v4 [quant-ph].

[12] M-D Choi, *Positive linear maps on C^*-algebras*. Canad. J. Math. **24**, 520-529 (1972).

[13] G M D'Ariano and P Lo Presti, *Imprinting a complete information about a quantum channel on its output state*. Phys. Rev. Lett. **91**, 047902 (2003).

[14] F Buscemi, *Comparison of Quantum Statistical Models: Equivalent Conditions for Sufficiency*. Comm. Math. Phys. **310**, 625–647 (2012).

[15] F Buscemi, *All Entangled States are Nonlocal*. Phys. Rev. Lett. **108**, 200401 (2012).

[16] G Smith, J A Smolin, and A Winter, *The quantum capacity with symmetric side channels*. IEEE Trans. Info. Theory **54**, 9, 4208-4217 (2008).

[17] F G S L Brandão and J Oppenheim, *The quantum one-time pad in the presence of an eavesdropper*. Phys. Rev. Lett. **108**, 040504 (2012).

[18] F G S L Brandão and J Oppenheim, *Public Quantum Communication and Superactivation*. IEEE Trans. Info. Theo. **59**, 2517 (2013).

[19] Graeme Smith, John A. Smolin, *Additive Extensions of a Quantum Channel*. Proc. of the IEEE Inf. Th. Workshop 2008, pp 368-372.

[20] E. Schrodinger, Proc. Camb. Phil. Soc. **31**, 555 (1935).