Selected Advances in Quantum Shannon Theory

Dedicated to the 100th Birthday of Claude E. Shannon

Nilanjana Datta (Statistical Laboratory, University of Cambridge, UK)

The last few years have witnessed various significant advances in quantum Shannon theory. In this article, we briefly review the salient features of three of them: a counterexample to the additivity conjecture, superactivation of the quantum capacity of a channel and one-shot quantum information theory. The first two pertain to information-transmitting properties of quantum channels whilst the third applies to a plethora of information-processing tasks, over and above information transmission.

The biggest hurdle in the path of information transmission is the presence of noise in communication channels, which can distort messages sent through them and necessitates the use of error-correcting codes. There is, however, a fundamental limit on the rate at which information can be transmitted reliably through a channel. The maximum rate is called the capacity of the channel and was originally evaluated in the so-called *asymptotic, memoryless (or i.i.d.) setting*. In this setting, it is assumed that the channel is: (*i*) available for an unlimited number of uses (say, n) and (*ii*) memoryless, i.e. there is no correlation in the noise acting on successive inputs to the channel. Classically, such a channel is modelled by a sequence of independent and identically distributed (i.i.d.) random variables. The capacity of the channel is the optimal rate at which information can be reliably transmitted through it in the asymptotic limit ($n \to \infty$).

The capacity of a memoryless classical channel was derived by Claude Shannon in his seminal paper of 1948 [1], which heralded the birth of the field of classical information theory. His *Noisy Channel Coding Theorem* gives an explicit expression for the capacity of a discrete memoryless channel $\mathcal{N}$. Such a channel can be completely described by its conditional probabilities $p_{Y|X}(y|x)$ of producing output y given input x, with X and Y denoting discrete random variables characterising the inputs and outputs of the channel. Shannon proved that the capacity $C(\mathcal{N})$ of such a channel is given by the formula

$$C(\mathcal{N}) = \max_{\{p_X(x)\}} I(X:Y), \tag{1}$$

where $I(X:Y)$ denotes the mutual information of the random variables X and Y, and the maximisation is over all possible input probability distributions $\{p_X(x)\}$.

In contrast to a classical channel, a quantum channel has many different capacities. These depend on various factors, e.g. on the type of information (classical or quantum) being transmitted, the nature of the input states (entangled or not), the nature of the measurements made on the outputs of the channel (collective or individual) and whether any auxiliary resources are available to assist the transmission. Auxiliary resources, like prior shared entanglement between the sender and the receiver, can enhance the capacities of a quantum channel. This is in contrast to the case of a classical channel, where auxiliary resources, such as shared randomness between the sender and the receiver, fail to enhance the capacity.

Let us briefly recall some basic facts about quantum channels. For simplicity of exposition, we refer to the sender as Alice and the receiver as Bob. A quantum channel $\mathcal{N}$ is mathematically given by a linear, completely positive trace-preserving (CPTP) map, which maps states (i.e. density matrices) ρ of the input quantum system A to states of the output system B. More generally, $\mathcal{N} \equiv \mathcal{N}^{A\to B} : \mathcal{B}(\mathcal{H}_A) \to \mathcal{B}(\mathcal{H}_B)$, where $\mathcal{H}_A$ ($\mathcal{H}_B$) denote the Hilbert spaces associated with the system A (B) and, in this article, they are considered to be finite-dimensional. By Stinespring's dilation theorem, any such quantum channel can be seen as an isometry followed by a partial trace, i.e. there is an auxiliary system E, usually referred to as the *environment*, and an isometry $U_\mathcal{N} : \mathcal{H}_A \to \mathcal{H}_B \otimes \mathcal{H}_E$, such that $\mathcal{N}(\rho) = \mathrm{Tr}_E\, U_\mathcal{N} \rho U_\mathcal{N}^\dagger$. This, in turn, induces the complementary channel $\mathcal{N}_c \equiv \mathcal{N}_c^{A\to E} : \mathcal{B}(\mathcal{H}_A) \to \mathcal{B}(\mathcal{H}_E)$ from the system A to the environment E, given by $\mathcal{N}_c(\rho) = \mathrm{Tr}_B\, U_\mathcal{N} \rho U_\mathcal{N}^\dagger$. Physically, the complementary channel captures the environment's view of the channel. A quantum channel is said to be *anti-degradable* if there exists a CPTP map $\mathcal{E} : \mathcal{B}(\mathcal{H}_E) \to \mathcal{B}(\mathcal{H}_B)$ so that the composition of the maps $\mathcal{N}_c$ and $\mathcal{E}$ satisfies the identity $\mathcal{N} = \mathcal{E} \circ \mathcal{N}_c$. So, an eavesdropper (Eve), who has access to the environment of the channel, can simulate the channel from A to B by locally applying the map $\mathcal{E}$. An anti-degradable channel has zero quantum capacity since it would otherwise violate the so-called *no-cloning theorem*, which forbids the creation of identical copies of an arbitrary unknown quantum state. This can be seen as follows. Suppose there is an encoding and decoding scheme for Alice to communicate quantum information reliably at a non-zero rate over such a channel. Then, by acting on the output that she receives by the CPTP map $\mathcal{D} \circ \mathcal{E}$, where $\mathcal{D}$ is the decoding map that Bob uses, Eve could obtain the quantum information sent by Alice. However, the ability for both Bob and Eve to obtain Alice's information violates the no-cloning theorem. Hence the quantum capacity of an anti-degradable channel must be zero. In contrast, a quantum channel is said to be degradable if there exists a CPTP map $\mathcal{E}' : \mathcal{B}(\mathcal{H}_B) \to \mathcal{B}(\mathcal{H}_E)$ such that $\mathcal{N}_c = \mathcal{E}' \circ \mathcal{N}$. In this case, Bob can simulate the complementary channel from A to E by locally applying the map $\mathcal{E}'$.

The problem of determining the different capacities of a quantum channel have only been partially resolved, in the sense that the expressions obtained for most of them thus far are regularised ones. They are therefore intractable and cannot be used to determine the capacities of a given channel in any effective way. If entanglement between inputs to successive uses of a quantum channel is not allowed, its capacity for transmitting classical information is given by an entropic quantity, $\chi^*(\mathcal{N})$, called its Holevo capacity [2]. The general classical capacity of a quantum channel, in the absence of auxiliary resources and without the above restriction, is given by the following regularised expression:

$$C(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n}\chi^*(\mathcal{N}^{\otimes n}). \tag{2}$$

Similarly, the capacity $Q(\mathcal{N})$ of a quantum channel for transmitting quantum information (in the absence of auxiliary resources) is also known [3] to be given by a regularised expression:

$$Q(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n} I_c(\mathcal{N}^{\otimes n}), \tag{3}$$

where, for any quantum channel $\widetilde{\mathcal{N}}$, $I_c(\widetilde{\mathcal{N}})$ is an entropic quantity referred to as its coherent information.

Another important capacity of a quantum channel is its private capacity $P(\mathcal{N})$, which is the maximum rate at which classical information can be sent through it in a way such that an eavesdropper, Eve, who has access to the environment of the channel, cannot infer the transmitted information. The private classical capacity $P(\mathcal{N})$ of a quantum channel is also given by the regularisation of an entropic quantity, which we denote $P^{(1)}(\mathcal{N})$. Unfortunately, these intractable, regularised expressions are in general useless for computing the actual capacities of a channel. Regarding the quantum capacity, an exception to this is provided by so-called degradable channels, for which the coherent information is additive and so the quantum capacity reduces to a single-letter formula. Other than the Holevo capacity, there are only a few other capacities which have a single-letter (and hence not-regularised) expression for any arbitrary quantum channel. The most important of these is the entanglement-assisted classical capacity [4], which is the maximum rate of reliable classical communication when Alice and Bob are allowed to make use of entangled states that they initially share.

An important property of the capacity of a classical channel is its additivity on the set of channels. Given two classical channels $\mathcal{N}_1$ and $\mathcal{N}_2$, the capacity of the product channel $\mathcal{N}_1 \otimes \mathcal{N}_2$ satisfies $C(\mathcal{N}_1 \otimes \mathcal{N}_2) = C(\mathcal{N}_1) + C(\mathcal{N}_2)$. In fact, many important questions in information theory can be reduced to the purely mathematical question of additivity of certain entropic functions on the set of channels. In particular, the regularised expressions for the classical, quantum and private capacities of a quantum channel $\mathcal{N}$ would reduce to tractable single-letter expressions if its Holevo capacity, coherent information and $P^{(1)}(\mathcal{N})$ were respectively additive. However, it has been proved that the coherent information and $P^{(1)}(\mathcal{N})$ are not necessarily additive for all channels. It was conjectured that the Holevo capacity of a quantum channel is indeed additive, i.e. for any two quantum channels $\mathcal{N}_1$ and $\mathcal{N}_2$,

$$\chi^*(\mathcal{N}_1 \otimes \mathcal{N}_2) = \chi^*(\mathcal{N}_1) + \chi^*(\mathcal{N}_2).$$

This conjecture is directly related to the important question: *'Can entanglement between successive input states boost classical communication through a memoryless quantum channel?'* The answer to this question is "no" if the Holevo capacity of the channel is additive, since in this case $C(\mathcal{N}) = \chi^*(\mathcal{N})$, i.e. the general classical capacity reduces to the classical capacity evaluated under the restriction of unentangled input states. The additivity conjecture had been proved for several channels (see, for example, [5] and references therein). However, proving that it is true for *all* quantum channels had remained an important open problem for more than a decade. Shor [6] provided useful insights into the problem by proving that the additivity conjecture for the Holevo capacity was equivalent to additivity-type conjectures for three other quantities arising in quantum information theory, in the sense that if any one of these conjectures is always true then so are the others. One of these conjectures concerns the additivity of the minimum output entropy (MOE) of a quantum channel, which is defined as

$$H_{\min}(\mathcal{N}) = \min_{\rho} H(\mathcal{N}(\rho)),$$

where, for any state σ, $H(\sigma) := -\operatorname{Tr}(\sigma \log \sigma)$ is its von Neumann entropy. The additivity conjecture for the MOE is that, for any pair of quantum channels $\mathcal{N}_1$, $\mathcal{N}_2$, the minimum entropy of the product channel $\mathcal{N}_1 \otimes \mathcal{N}_2$ satisfies

$$H_{\min}(\mathcal{N}_1 \otimes \mathcal{N}_2) = H_{\min}(\mathcal{N}_1) + H_{\min}(\mathcal{N}_2). \tag{4}$$

Note that we always have $\leq$ in (4). This can be seen by considering the product state $\rho_1 \otimes \rho_2$ as input to $\mathcal{N}_1 \otimes \mathcal{N}_2$, with ρ_1 and ρ_2 being the minimisers for MOEs of $\mathcal{N}_1$ and $\mathcal{N}_2$ respectively. The conjecture amounts to the claim that we cannot get a smaller MOE by entangling the inputs to $\mathcal{N}_1 \otimes \mathcal{N}_2$.

These longstanding additivity conjectures were finally resolved in 2008 by Hastings [7], who built on prior work by Hayden and Winter [8]. He proved the existence of a pair of channels for which the above conjecture is false. By Shor's equivalence, this in turn implied that all the additivity conjectures (including that for the Holevo capacity) are false. Hence, we can conclude that there exist quantum channels for which using entangled input states can indeed enhance the classical capacity.

The product channel considered by Hastings has the form $\mathcal{N} \otimes \overline{\mathcal{N}}$, where $\mathcal{N}$ is a special channel called a *random unitary channel*, and $\overline{\mathcal{N}}$ is its complex conjugate. This means that there are positive numbers $\nu_1, \nu_2, \ldots, \nu_d$, with $\sum_{i=1}^{d} \nu_i = 1$, and unitary $n \times n$ matrices $U_1, U_2, \ldots, U_d$, chosen at random with respect to the Haar measure, such that for any input state ρ,

$$\mathcal{N}(\rho) = \sum_{i=1}^{d} \nu_i U_i \rho U_i^\dagger \quad ; \quad \overline{\mathcal{N}}(\rho) = \sum_{i=1}^{d} \nu_i \overline{U}_i \rho \overline{U}_i^\dagger.$$

The probabilities ν_i are chosen randomly and depend on the integers n and d, where n is the dimension of the input space of the channel and d is the dimension of its environment. Hastings' main result is that for n and d large enough, there are random unitary channels for which $H_{\min}(\mathcal{N} \otimes \overline{\mathcal{N}}) < H_{\min}(\mathcal{N}) + H_{\min}(\overline{\mathcal{N}})$, thus disproving (4).

A key ingredient of Hastings' proof is the relative values of the dimensions, namely $n >> d >> 1$. The details of Hastings' original argument were elucidated later by Fukuda, King and Moser [9]. These authors also derived explicit lower bounds to the input, output and environment dimensions of a quantum channel for which the additivity conjecture is violated. A simplified proof of Hastings' result was given by Brandao and Horodecki [10] in the framework of concentration of measure. They also proved non-additivity for the overwhelming majority of channels consisting of a Haar random isometry followed by partial trace over the environment, for an environment dimension much bigger than the output dimension, thus extending the class of channels for which additivity can be shown to be violated. Remarkably, in 2010, Aubrun, Szarek and Werner [11] proved that Hastings' counterexample can be readily deduced from a version of *Dvoretzky's theorem*, which is a fundamental result of Asymptotic Geometric Analysis – a field of mathematics concerning the behaviour of geometric parameters associated with norms in $\mathbb{R}^n$ (or equivalently, with convex bodies) when n becomes large. However, the violation to additivity in Hastings' example is numerically small and the question of how strong a violation of additivity is possible is the subject of active research.

The year 2008 also saw the discovery of a startling phenomenon in quantum information theory, again related to the question of additivity of capacities. Smith and Yard [12] proved that there are pairs of quantum channels each having zero quantum capacity but which have a non-zero quantum capacity when used together. Hence, even though each channel in such a pair is by itself useless for sending quantum information, they can be used together to send quantum information reliably. This phenomenon was termed "superactivation", since the two channels somehow "activate" each other's hidden ability to transmit quantum information. Superactivation is a purely quantum phenomenon because classically if two channels have zero capacity, the capacity of the joint channel must also be zero. This follows directly from the additivity of the capacity of a classical channel, which in turn ensures that the capacity of a classical channel is an intrinsic measure of its information-transmitting properties. In the quantum case, in contrast, the possibility of superactivation implies that the quantum capacity of a channel is strongly non-additive and does not adequately characterise its ability to transmit quantum information, since the usefulness of a channel depends on what other channels are also available. A particular consequence of this phenomenon is that the set of quantum channels with zero quantum capacity is not convex.

Superactivation of quantum capacity continues to be the subject of much research and is still not completely understood. However, it seems to be related to the existence of channels, called "private Horodecki channels", which have zero quantum capacity but positive private capacity. The key ingredient of Smith and Yard's proof of superactivation is a novel relationship between two different capacities of a quantum channel $\mathcal{N}$, namely, its private capacity $P(\mathcal{N})$ and its assisted capacity $Q_A(\mathcal{N})$. The latter is the quantum capacity of the product channel $\mathcal{N} \otimes \mathcal{A}$, where $\mathcal{A}$ is a *symmetric channel*. Such a channel maps symmetrically between its output and its environment, i.e. for any input state ρ, the joint state $\sigma_{BE} := U_{\mathcal{A}} \rho U_{\mathcal{A}}^\dagger$ of the output and the environment after the action of the channel $\mathcal{A}$ is invariant under the interchange of B and E. A symmetric side channel is anti-degradable and hence has zero quantum capacity. Smith and Yard proved that

$$Q_{\mathcal{A}}(\mathcal{N}) \geq \frac{1}{2} P(\mathcal{N}).$$

This in turn implies that any private Horodecki channel, $\mathcal{N}_H$, has a positive assisted capacity and hence the two zero-quantum-capacity channels $\mathcal{N}_H$ and $\mathcal{A}$ exhibit superactivation:

$$Q_A(\mathcal{N}_H) = Q(\mathcal{N}_H \otimes \mathcal{A}) > 0.$$

The particular symmetric side channel that Smith and Yard considered was a 50% *erasure channel*, which, with equal probability, faithfully transmits the input state or outputs an erasure flag.

Later, Brandao, Oppenheim and Strelchuk [13] proved that superactivation even occurs for pairs of channels $(\mathcal{N}_H, \mathcal{N})$ where $\mathcal{N}$ is anti-degradable but not necessarily symmetric. Specifically, they proved the occurrence of superactivation for two different choices of $\mathcal{N}$: (i) an erasure channel that outputs an erasure flag with probability $p \in [1/2, 1)$ and faithfully transmits the input state otherwise; and (ii) a depolarising channel that completely randomises the input state with probability $p \in [0, 1/2]$ and faithfully transmits the input state otherwise. It is known that the output of any arbitrary quantum channel can be mapped to that of a depolarising channel by an operation known as "twirling". The latter consists of Alice applying some randomly chosen unitary on the input state before sending it through the channel and informing Bob as to which unitary operator U she used, with Bob subsequently acting on the output state of the channel by the inverse operator $U^\dagger$. This special feature of the depolarising channel and the fact that it can be used for superactivation, suggests that superactivation is a rather generic effect. Superactivation has also been proven for other capacities of a quantum channel (see, for example, [14] and references therein), namely its zero-error classical and quantum capacities, which are, respectively, the classical and quantum capacities evaluated under the requirement that the probability of an error being incurred in transmitting the information is strictly zero (and doesn't just vanish asymptotically).

All the capacities mentioned above were originally evaluated in the limit of asymptotically many uses of a memoryless channel. In fact, optimal rates of most information-processing tasks, including transmission and compression of information, and manipulation of entanglement, were originally evaluated in the asymptotic, memoryless setting. As mentioned above, in this setting, one assumes that there is no correlation in successive uses of resources (e.g. information sources, channels and entanglement resources) employed in the tasks, and one requires the tasks to be achieved perfectly in the limit of asymptotically many uses of the resources. These asymptotic rates, e.g. the various capacities discussed above, are seen to be given in terms of entropic functions that can all be derived from a single parent quantity, namely, the quantum relative entropy.

In reality, however, the assumption of resources being uncorrelated and available for an unlimited number of uses is not necessarily justified. This is particularly problematic in cryptography, where one of the main challenges is dealing with an adversary who might pursue an *arbitrary* (and unknown) strategy. In particular, the adversary might manipulate resources (e.g. a communications channel) and introduce undesired correlations. A more general theory of quantum information-processing tasks is instead obtained in the so-called *one-shot scenario* in which resources are considered to be finite and possibly correlated. Moreover, the information-processing tasks are required to be achieved only up to a finite accuracy, i.e. one allows for a fixed, non-zero but small error tolerance. This also corresponds to the scenario in which experiments are performed since channels, sources and entanglement resources available for practical use are typically finite and correlated, and transformations can only be achieved approximately.

The last few years have witnessed a surge of research leading to the development of *one-shot quantum information theory*. The birth of this field can be attributed to Renner (see [15] and references therein) who introduced a mathematical framework, called the *smooth entropy framework,* which facilitated the analysis of information-processing tasks in the one-shot scenario. He and his collaborators introduced new entropy measures of states, called *smooth min- and max-entropies*, which depend on a parameter (say, ε), called the smoothing parameter. The smooth entropies $H^{\varepsilon}_{\min}(\rho)$ and $H^{\varepsilon}_{\max}(\rho)$ of a state ρ can be defined as optimisations of the relevant non-smooth quantities, the (non-smooth) min- and max-entropies, over a ball $B^{\varepsilon}(\rho)$ of neighbouring states, which are at a distance of at most ε from ρ, measured in an appropriate metric. For a bipartite state ρ_{AB}, they also define conditional min- and max-entropies.

Subsequently, it was proved (see, for example, [16]) that these conditional and unconditional smooth min- and max-entropies characterise the optimal rates of various information-processing tasks in the one-shot scenario, with the smoothing parameter corresponding to the allowed error tolerance. For example, the one-shot ε-error quantum capacity of a channel, which is the maximum amount of quantum information that can be transmitted over a single use of a quantum channel with an error tolerance of ε, has been proven to be given in terms of a smooth conditional max-entropy [22, 17]. Note that a single use of a channel can itself correspond to a finite number of uses of a channel with arbitrarily correlated noise. Hence the one-shot analysis indeed includes the consideration of finite, correlated resources. Furthermore, one-shot rates of all the different information-processing tasks studied thus far readily yield the corresponding known rates in the asymptotic limit, in the case of uncorrelated (i.e. memoryless) resources. Moreover, they also yield asymptotic rates of tasks involving correlated resources via the so-called Quantum Information Spectrum method (see, for example, [18] and references therein). Hence, one-shot quantum information theory can be viewed as the fundamental building block of quantum information theory and its development has opened up various new avenues of research.

In [20], we defined a generalised relative entropy called the *max-relative entropy*, from which the min- and max-entropies can be readily obtained, just as the ordinary quantum (i.e. von Neumann) entropies are obtained from the quantum relative entropy. Hence, the max-relative entropy plays the role of a parent quantity for optimal rates of various information-processing tasks in the one-shot scenario, analogous to that of the quantum relative entropy in the asymptotic, memoryless scenario. Moreover, it has an interesting operational interpretation, being related to the optimal Bayesian error probability in determining which one, of a finite number of known states, a given quantum system is prepared in. The max-relative entropy also leads naturally to the definition of an entanglement monotone, which is seen to have an interesting operational interpretation in the context of entanglement manipulation [19]. The different information-processing tasks in the one-shot scenario were initially studied separately. However, we subsequently proved [22] that a host of these tasks can be related to each other and conveniently arranged in a family tree, thus yielding a unifying mathematical framework for analysing them. Recently, we introduced a two-parameter family of generalised relative entropies, called the $\alpha - z$ relative Rényi entropies, from which the various different relative entropies (including the quantum relative entropy and the max-relative entropy) that arise in quantum information theory can be derived. This family provides a unifying framework for the analysis of properties of these different relative entropies, which are both of mathematical interest and of operational significance.

References

[1] C. E. Shannon, *Bell System Technical Journal*, **27**, 379 (1948).
[2] A. S. Holevo, *IEEE Trans. Inf. Theory*, **44**, 269 (1998); B. Schumacher & M. D. Westmoreland, *Phys. Rev. A*, **56**, 131 (1997).
[3] I. Devetak, *IEEE Trans. Inf. Theory*, **51**, **44** (2005); S. Lloyd, *Phys. Rev. A*, **55**, 1613 (1997); P. W. Shor, MSRI Workshop on Quantum Computation (2002).
[4] C. H. Bennett, P. W. Shor, J. A. Smolin & A. V. Thapliyal, *IEEE Trans. Inf. Theory*, **48**, 2637 (2002); A. S. Holevo, *J. Math. Phys.*, **43**, 4326 (2002).
[5] C. King, *J. Math. Phys.* **43**, 4641 (2002); *IEEE Trans. Inf. Theory*, **49**, 221, 2003; C. King, K. Matsumoto, M. Nathanson and M. B. Ruskai, *Markov Process and Related Fields*, **13**, 391 (2007); N. Datta, M. Fukuda and A. S. Holevo, *Quan. Inf. Proc.*, **5**, 179 (2006).
[6] P. W. Shor, *Comm. Math. Phys.* **246**, 453 (2004).
[7] M. B. Hastings, *Nature Physics* **5**, 255 (2009).
[8] P. Hayden & A. Winter, *Comm. Math. Phys.* **284**, 263 (2008).
[9] M. Fukuda, C. King & D. Moser, *Comm. Math. Phys.* **296**, 111 (2010). 2007.
[10] F. G. S. L. Brandao & M. Horodecki, *Open Syst. Inf. Dyn.* **17**, 31 (2010).
[11] G. Aubrun, S. Szarek & E. Werner, *Comm. Math. Phys.* **305**, 85 (2011).
[12] G. Smith & J. Yard, *Science* **321**, 1812 (2008); G. Smith, J. A. Smolin, & J. Yard, *Nature Photonics*, **5**, 624 (2011).
[13] F. G. S. L. Brandao, J. Oppenheim & S. Strelchuk, *Phys. Rev. Lett.* **108**, 040501 (2012).

[14] J. Chen, T. S. Cubitt, A. W. Harrow & G. Smith, *Phys. Rev. Lett.* **107**, 250504 (2011); J. Chen, T. S. Cubitt & A. W. Harrow, *IEEE Trans. Inf. Th.*, **57**, 8114 (2011).
[15] R. Renner, *PhD thesis*, ETH Zurich, 2005; R. Renner & R. Koenig, *Proc. of TCC* 2005, LNCS, Springer, **3378** (2005).
[16] F. Buscemi & N. Datta, *J. Math. Phys.*, **51**, 102201, 2010; F. Buscemi & N. Datta, *Phys. Rev. Lett.* **106**, 130503 (2011), F. Buscemi & N. Datta, *IEEE Trans. Inf. Th.*, **59**, 1940 (2013); M. Berta, M. Christandl & R. Renner, *Commun. Math. Phys.*, **306**, 579 (2011); L. Wang & R. Renner, *Phys. Rev. Lett.*, **108**, 200501 (2012); J. M. Renes & R. Renner, *IEEE Trans. Inf. Th.*, **58**, 1985 (2012); N. Datta & M. H. Hsieh, *IEEE Trans. Inf. Th.*, **59**, 1929 (2013).
[17] F. Buscemi & N. Datta, *IEEE Trans. Inf. Theory*, **56**, 1447 (2010).
[18] N. Datta & R. Renner *IEEE Trans. Inf. Theory* **55**, 2807 (2009).
[19] F. Brandao & N. Datta, *IEEE Trans. Inf. Theory*, **57**, 1754 (2011).
[20] N. Datta, *IEEE Trans. Inf. Theory*, **55**, 2816 (2009).
[21] N. Datta & M.-H. Hsieh, *New J. Phys.*, **13** 093042 (2011).
[22] K. M. R. Audenaert & N. Datta *Jour. Math. Phys.*, **56**, 022202 (2015).

Nilanjana Datta [n.datta@statslab.cam.ac.uk] is an affiliated lecturer of the Statistical Laboratory, Centre for Mathematical Sciences, University of Cambridge, and a fellow of Pembroke College. She completed her PhD in mathematical physics at ETH Zurich in 1996. She has been working on quantum information theory since 2001 and has written papers on various topics in this field. These include quantum channels and the additivity problem, quantum data compression, perfect transfer of quantum states and entanglement theory. In the last few years, her research has focused on developing one-shot quantum information theory, which concerns the analysis of information processing tasks involving finite, correlated resources.