BOOK REVIEWS

BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 58, Number 2, April 2021, Pages 277–281
https://doi.org/10.1090/bull/1706
Article electronically published on August 19, 2020

Alice and Bob meet Banach: The interface of asymptotic geometric analysis and quantum information theory, by Guillaume Aubrun and Stanisław Szarek, Mathematical Surveys and Monographs, Vol. 223, American Mathematical Society, Providence, RI, 2017, xxi+414 pp., ISBN 978-1-470-43468-7, US$ 116.00

Broadly speaking, the fundamental role of any computational device is to store and transmit information. For the "classical" computers we use in our everyday lives, the mathematical framework that describes the transmission, processing, extraction, and utilization of information is *information theory.* The field of information theory was pioneered by Claude E. Shannon in his seminal 1948 paper [9]. It is difficult to overestimate the influence that information theory has had on modern computation. For example, it describes the fundamental limits and capabilities of data compression (e.g., JPEG image encoding), wireless communications, intenet security protocols, and so on.

One of the early achievements of information theory was Shannon's noisy channel coding theorem [9], which provides a computable expression for the *capacity* of a noisy communications channel. More precisely, imagine we have two parties, Alice and Bob, and suppose that Alice (the sender) wishes to send messages over some noisy medium (e.g., over a cellular network) to Bob (the receiver). Alice will posses a finite alphabet A of possible input messages, and Bob will receive at his end a message from an alphabet of possible outputs B. A (discrete, memoryless) noisy channel $\Phi : A \to B$ is then modeled by a conditional probability distribution $(p(b|a))_{a\in A, b\in B}$, so that $p(b|a)$ indicates the probability that Bob receives message $b \in B$ given that Alice sent $a \in A$. The *capacity* $C(\Phi)$ of a noisy channel Φ is the optimal rate at which information can be reliably transmitted through the channel (measured in bits-per-channel use per second). To compute the capacity $C(\Phi)$, consider a random variable $X \in A$ with probability distribution $p_X \in \ell^1(A)$. Then the distribution of the output random variable $Y \in B$ has distribution $p_Y \in \ell^1(B)$ given by $p_Y(b) = \sum_{a\in A} p(b|a)p_X(a)$. Given X, Y as above, we can compute the *mutual information* $I(X;Y)$ which is given by the formula $I(X;Y) = H(X) + H(Y) - H(X,Y)$. Here $H(Z) = -\sum_z p_Z(z)\log p_Z(z)$ is the Shannon entropy of a finite random variable Z with distribution p_Z. Finally, the capacity $C(\Phi)$ can then be computed by the convex optimization problem,

$$C(\Phi) = \max_{p_X} I(X;Y). \tag{1}$$

Over the past few decades one of the major goals of computer science has been that of building a practical *quantum computer*, i.e., a computational device that can store and manipulate *quantum* information and states in quantum mechanical systems. The reason for the high level of interest in quantum computers is not that that they are expected to solve more computational problems (in fact by the Church–Turing thesis any computation performed by a quantum computer can also be performed on a classical computer). Instead it is that quantum computers have the potential to provide exponential speedup when it comes to time complexity of certain algorthims. A famous example here is Shor's polynomial time quantum algorithm for factoring integers [10]. If such an algorithm could be reliably implemented on a quantum computer, this would provide a means to decrypt RSA-encrypted communications—a serious threat to modern-day cryptosystems.

As one might expect, in the world of quantum computing there is a quantum analogue of Shannon's information theory called *quantum information theory* (*QIT*). The goal of this rapidly developing field is to provide the mathematical foundation to describe the fundamental limits of processing both classical and quantum information. In the monograph under review [3], the central focus is the subject of quantum information theory and its intriguing interactions with the subject of *asymptotic geometric analysis* (*AGA*), that is, the geometric study of finite-dimensional Banach spaces and convex bodies in their large dimension limit. This includes deep applications of random matrix theory, free probability, operator systems, harmonic analysis, concentration of measure phenomena, representation theory, and so on.

To get a taste of how ideas from AGA all fit together to provide deep insight into QIT problems, let us first review some basic notions in quantum mechanics and QIT. A (finite) *quantum system* is described by a finite-dimensional complex Hilbert space H. A (*pure*) *state* of a quantum system H is described by a rank-1 projection $\rho = |\xi\rangle\langle\xi| \in \mathrm{End}(H)$. The convex hull of all pure states of H is denoted by $D(H)$. Elements of $D(H)$ are the *mixed quantum states* of H and are precisely the positive semidefinite trace-1 elements of $\mathrm{End}(H)$. The analogy to keep in mind is that for a classical system with finite alphabet A, the canonically associated quantum system is the Hilbert space $\ell^2(A)$ with distinguished orthonormal basis $(|\delta_a\rangle)_{a\in A}$ given by the Dirac functions on A. Classical states of A (i.e., elements $a \in A$) are then given by the pure quantum states $(|\delta_a\rangle\langle\delta_a|)_{a\in A}$, and the mixed states correspond to the diagonal elements of $D(\ell^2(A))$ with respect to our fixed basis, i.e., probability density functions on A. In this way, the classical world naturally embeds into the quantum world. In QIT, a noisy communications channel can be thought of as certain "physically realizable" operation that takes mixed quantum states of one quantum system H_A to mixed quantum states of another quantum system H_B. Mathematically, this is described by a *quantum channel*: a linear completely positive trace-preserving map $\Phi : \mathrm{End}(H_A) \to \mathrm{End}(H_B)$. Again, classical channels embed into this framework as those quantum channels with the additional property that they send diagonal states to diagonal states with respect to some fixed orthonormal bases. Perhaps the most important phenomenon in quantum information theory (and, more generally, quantum physics) that is not present in the classical world is *entaglement* in multipartite quantum systems. Let us consider the bipartite setup here for simplicity: A *bipartite quantum system* is simply a quantum system of the form $H_{AB} = H_A \otimes H_B$. We call the H_A (resp., H_B) subspace the A (resp., B) subsystem. A bipartite quantum state $\rho \in D(H_A \otimes H_B)$ is *separable* if ρ is a convex combination of product states $\rho_A \otimes \rho_B$. If ρ is not seprable, we call ρ an *entangled* state. The prototypical example of an entangled pure state is the *Bell state* $\rho = |\xi\rangle\langle\xi| \in D(\mathbb{C}^2 \otimes \mathbb{C}^2)$ with $\xi = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Bell states and other entangled states form an essential resource in just about any quantum algorithm, including quantum teleportation and superdense coding [7], Shor's prime factorization algorithm [10], and also in the theory of nonlocal games [3, Chapter 11], [8].

Returning to the connection between AGA and QIT, it is clear from the previous paragraph that the mathematical structures (e.g., complete positivity, convexity, finite-dimensional operator algebra) that describe QIT trivially belong within the framework of (asymptotic) geometric analysis. However (and this is one of the main goals of the monograph [3]), this connection runs so much deeper. It turns out that many physically relevant and practical questions arising in QIT can be tackled systematically and efficiently with powerful methods from AGA.

One particularly beautiful example of this connection (discussed in great detail in Chapter 8 of the book under review) is the additivity problem for the minimum output entropy for quantum channels. Given a quantum channel $\Phi : \mathrm{End}(H_A) \to \mathrm{End}(H_B)$, the *minimum output entropy* (*MOE*) of Φ is the quantity

$$S_{\min}(\Phi) = \min_{\rho \in D(H_A)} S(\Phi(\rho)),$$

where $S(\rho) = -\mathrm{Tr}(\rho \log \rho)$ is the *von Neumann entropy* of a quantum state ρ. It is not hard to see that one always has, for any pair of channels Φ, Ψ, the inequality $S_{\min}(\Phi \otimes \Psi) \leq S_{\min}(\Phi) + S_{\min}(\Psi)$. A key problem in QIT dating back to the early 2000s was to determine if strict inequality can ever occur: Are there channels for which the MOE is not additive with respect to tensor products? The reason for the interest in the MOE additivity problem stems from another important QIT problem: How does one compute the *classical information capacity* $C(\Phi)$ of a quantum channel? Unlike in the classical world of Shannon, the capacity of a general quantum channel Φ is not known to have a nice computable expression such as what we saw in (1). Instead, it is given by a (computationally impactical) regularized expression of the form

$$C(\Phi) = \lim_{n \to \infty} n^{-1} \chi(\Phi^{\otimes n}),$$

where $\chi(\cdot)$ is a certain expression known as the *Holevo capacity* (or one-shot capacity) of a channel [5]. Thus an essential question was whether or not the regularization in the above formula was really needed. The necessity for regularization was shown by Shor [11] to be equivalent to the existence of channels that are not MOE additive. The existence of quantum channels which fail to be MOE additive was first established by Hastings [4] using random Haar-distributed unitary quantum channels and a certain concentration of measure results on large unitary groups. In the monograph [3], the authors carefully explain how the existence of such channels can be seen as a consequence of the Dvoretzky–Milman theorem for Lipshitz functions [3, Theorem 7.15]. The ideas presented here are based upon earlier works of the authors together with E. Werner [1, 2]. The key idea is to use the Dvoretzky–Milman theorem to assert the existence of Haar-distributed random subspaces $W \subset \mathbb{C}^k \otimes \mathbb{C}^d$ in which every pure state associated to the subspace W is almost maximally entangled. More precisely, one seeks subspaces $W \subset \mathbb{C}^k \otimes \mathbb{C}^d$ for which the *entanglement entropy* $E(|\xi\rangle) := S(\mathrm{id} \otimes \mathrm{Tr})(|\xi\rangle\langle\xi|))$ is essentially uniformly bounded below by $\log\left(\frac{kd}{\dim W}\right)$ for all unit vectors $|\xi\rangle \in W$. Applying the appropriate version of the Dvoretzky–Milman theorem to the Lipschitz funtion $E(\cdot)$ yields the existence of such W (for suitably chosen $d, k, \dim W \to \infty$). Such a random subspace can then be used to easily produce a pair of random quantum channels witnessing a MOE additivity violation. The above example is of course just one instance of many remarkable achievements in QIT which use deep methods of AGA in an essential way, but I feel that it is a good representative of the general theme and flavor of the AGA-QIT interactions that are at the heart of this book.

This book is divided into into three main parts. The first part, Alice and Bob: Mathematical aspects of quantum information theory, introduces basic terminology and mathematical concepts present in both QIT and geometric functional analysis. Topics covered include normed spaces, basic convex analysis, quantum systems, states, multipartite systems, quantum channels, common cones in QIT, and an overview of basic quantum mechanical principles for mathematicians. The second part, Banach and his spaces: Asymptotic geometric analysis miscellany, dives deeper into the main results of AGA that play a big role in QIT. Topics include convexity and classical inequalities for convex bodies, metric entropy and concentration of measure phenomena, Gaussian processes, and random matrices. These ideas all come together in the analysis of sections of high-dimensional convex bodies, proving the Johnson–Lindenstrauss lemma and various forms of Dvoretsky's theorem. The third and final part of the text, The meeting: AGA and QIT, brings all of the ideas of AGA introduced previously to bear on problems in QIT. In particular, Chapter 8 is devoted to the study of entanglement of random pure states in high dimensions. This is the key to the application of Dvoretsky's theorem in the study of MOE additivity problems for quantum channels. Chapter 9 studies the convex geometry (e.g., volume and mean width estimates) of spaces of mixed quantum states, and their subsets of PPT and separable states. Chapter 10 focuses on random quantum states and applies the volume and mean width results of Chapter 9 to study the probability of a random pure state on $\mathbb{C}^d \otimes \mathbb{C}^d$ to be entangled/separable. Chapter 11 focuses on another beautiful connection between functional analysis and QIT: the Bell and Grothendieck–Tsirelson inequalities. This connection is presented from the perspective of local vs. quantum correlation matrices and the famous CHSH inequality. This chapter also touches on the connection between Bell-type inequalities and the currently very hot topic of nonlocal games (see [6] for a very recent and spectacular application to operator algebras). The final Chapter 12 focuses on POVMs and gives a brief intoduction to the (currently still open) distillability problem in QIT: Given two bipartite states ρ, σ, is it always possible to convert (multiple copies of ρ) to a state which is arbitrarily close to σ via a so-called LOCC quantum channel? The text ends with several appendices providing some extra background material and references that are used throughout the text.

In summary, the monograph [3] is extremely well written and loaded with useful results and techniques—both for persons working in QIT or functional analysis. This book could be used for multiple purposes—for example as a general reference for researchers, as a broad graduate course in AGA with QIT applications, or as an introduction to the mathematics of QIT for graduate students in functional analysis and physics. I very highly recommend this book.

References

[1] G. Aubrun, S. Szarek, and E. Werner, *Nonadditivity of Rényi entropy and Dvoretzky's theorem*, J. Math. Phys. **51** (2010), no. 2, 022102, 7, DOI 10.1063/1.3271044. MR2605015

[2] G. Aubrun, S. Szarek, and E. Werner, *Hastings's additivity counterexample via Dvoretzky's theorem*, Comm. Math. Phys. **305** (2011), no. 1, 85–97, DOI 10.1007/s00220-010-1172-y. MR2802300

[3] G. Aubrun and S. J. Szarek, *Alice and Bob meet Banach: The interface of asymptotic geometric analysis and quantum information theory*, Mathematical Surveys and Monographs, vol. 223, American Mathematical Society, Providence, RI, 2017. MR3699754

[4] M. B. Hastings, *Superadditivity of communication capacity using entangled inputs*, Nat. Phys., **255** (2009), no. 5.

[5] A. S. Holevo, *Some estimates for the amount of information transmittable by a quantum communications channel* (Russian), Problemy Peredači Informacii **9** (1973), no. 3, 3–11. MR0456936

[6] Z. Ji, A. Natarajan, T. Vidick, J. Wright, and H. Yuen, MIP* = RE, preprint, arXiv:2001.04383 (2020).

[7] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*, Cambridge University Press, Cambridge, 2000. MR1796805

[8] C. Palazuelos and T. Vidick, *Survey on nonlocal games and operator space theory*, J. Math. Phys. **57** (2016), no. 1, 015220, 41, DOI 10.1063/1.4938052. MR3446943

[9] C. E. Shannon, *A mathematical theory of communication*, Bell System Tech. J. **27** (1948), 379–423, 623–656, DOI 10.1002/j.1538-7305.1948.tb01338.x. MR26286

[10] P. W. Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM Rev. **41** (1999), no. 2, 303–332, DOI 10.1137/S0036144598347011. MR1684546

[11] P. W. Shor, *Equivalence of additivity questions in quantum information theory*, Comm. Math. Phys. **246** (2004), no. 3, 453–472, DOI 10.1007/s00220-003-0981-7. MR2053939

Michael Brannan
Department of Mathematics, Mailstop 3368
Texas A&M University,
College Station, Texas 77843-3368
Email address: mbrannan@math.tamu.edu