Leaking information to gain entanglement via log-singularities *

Vikesh Siddhu†

Introduction—Confirmed experimentally [1] via violation of Bell type inequalities [2,3] and used for insights across disciplinary boundaries [4–6], entanglement is a distinctly non-classical resource. This resource is believed to play a non-trivial role in quantum computing. When used for communication [7,8] , it can provide unconditional security [9–11] and reduce classical communication complexity [12–14]. As a result, strong efforts are being made [15–18] for intermediate and large scale [19,20] use of quantum entanglement. However, these efforts are hindered by the susceptibility of entanglement to noise. It is critical to devise protocols and find maximum rates for protecting entanglement from noise.

General set-ups for protecting entanglement from noise described by a quantum channel $\mathcal{B}$ can be roughly described as follows. Suppose one has n copies of a quantum system a, and these systems are affected by an independent and identically distributed (i.i.d.) noise process, each described by the channel $\mathcal{B} : a \mapsto b$. A general task to protect an unknown pure state ψ_{RA}, entangled between a k qubit system A and an inaccessible reference R, can allow an arbitrary input encoding $\mathcal{E}_n : A \mapsto a^{\otimes n}$ and output decoding $\mathcal{D}_n : b^{\otimes n} \mapsto B$ across n joint channel uses $\mathcal{B}^{\otimes n}$. These encoding-decoding maps are to ensure that the state $\phi_{RB} = \mathcal{D}_n \circ \mathcal{B}^{\otimes n} \circ \mathcal{E}_n(\psi_{RA})$ protects entanglement with R, i.e, it is ϵ_n close to ψ_{RA}. This task is said to be achievable at a rate k/n when one can force ϵ_n to vanish as $n \mapsto \infty$. The maximum achievable rate of this entanglement protection task is given by the quantum capacity $\mathcal{Q}(\mathcal{B})$ of the channel $\mathcal{B}$.

The quantum capacity is also the highest rate for any quantum error correction code designed to recover quantum information affected by noise $\mathcal{B}$. Successful quantum error correction does not leak any information to the channel's environment. Thus a channel's private capacity $\mathcal{P}$ [21] to send classical information hidden from the channel's environment is bounded from below by its quantum capacity. The private capacity $\mathcal{P}(\mathcal{B})$ also equals the maximum rate for distributing a secret key by sending quantum states over a channel $\mathcal{B}$ whose complement $\mathcal{C}$ goes to an eavesdropper. Due to their central importance, computing and understanding quantum capacities is a central task of quantum information theory.

The best way to understand quantum capacities is rooted in Shannon's [22] original recipe for finding the capacity $C(N)$ of a noisy classical channel N. The recipe's key ingredient is $C^{(1)}(N)$, the maximum mutual information between the channel input variable and its image under the channel. A random coding argument shows that $C^{(1)}(N)$ is an achievable rate, i.e., $C^{(1)}(N) \leq C(N)$ and over k joint uses of N, $\lim_{k \mapsto \infty} C^{(1)}(N^{\times k})/k \leq C(N)$. The converse theorem, $C(N) \leq \lim_{k \mapsto \infty} C^{(1)}(N^{\times k})/k$ is established using Fano's inequality to obtain a matching upper and lower bound on $C(N)$. Finally, additivity, i.e, for any two channels N and N' used together $C^{(1)}(N' \times N)$ is $C^{(1)}(N') + C^{(1)}(N)$, reduces these bounds to an elegant one-letter formula $C(N) = C^{(1)}(N)$. Given that $C(N)$ is the ultimate limit for sending classical data across infinitely many uses of N, this one letter formula is surprising.

Expressions for quantum capacities are found in a similar way. For quantum and private capacities the respective quantum analogs of the key classical ingredient $C^{(1)}$, are the coherent information $\mathcal{Q}^{(1)}$ [23], and private information $\mathcal{P}^{(1)}$ [21]. Each quantity $\mathcal{Q}^{(1)}$ and $\mathcal{P}^{(1)}$ gives an achievable rate for its respective task. Like $C^{(1)}$, each of these quantum analogs comes from random coding arguments, however, unlike $C^{(1)}$, all of them are non-additive [24–28]. This non-additivity (see (1) for a precise definition) is remarkable. It presents an opportunity to find strategies for sending

*Two full papers, one on leakage and another on log-singularities, are included with this submission

† *Quantum Computing Group, Carnegie Mellon University:* vsiddhu@andrew.cmu.edu

information across quantum channels at rates which surpass naive random coding rates. Indeed a variety of strategies have been explored: structured quantum codes can sometimes improve upon $\mathcal{Q}^{(1)}$ [29, 30], and carefully crafted private codes can surpass $\mathcal{P}^{(1)}$ in certain cases [31].

While non-additivity brings new opportunities, it also creates challenges. For instance the best known formulas for quantum capacities of general channels are multi-letter expressions. Such expressions are hard to evaluate since they may require an intractable maximization of a non-convex function over an infinite number of variables. One such non-convex function is the coherent information of a channel $\mathcal{B}$ at an input density operator ρ, $\Delta(\mathcal{B}, \rho) := S(\mathcal{B}(\rho)) - S(\mathcal{C}(\rho))$, where $S(\rho) = -\text{Tr}(\rho \log \rho)$ is the von-Neumann entropy. The maximum of $\Delta(\mathcal{B}, \rho)$ over ρ gives the channel coherent information $\mathcal{Q}^{(1)}(\mathcal{B})$. Since $\mathcal{Q}^{(1)}$ is non-additive, i.e., for any two channels $\mathcal{B}$ and $\mathcal{B}'$ the inequality,

$$\mathcal{Q}^{(1)}(\mathcal{B} \otimes \mathcal{B}') \geq \mathcal{Q}^{(1)}(\mathcal{B}) + \mathcal{Q}^{(1)}(\mathcal{B}'), \tag{1}$$

can be strict, one must regularize the n-letter coherent information to obtain a multi-letter formula for the quantum capacity: for any channel $\mathcal{B}$, $\mathcal{Q}(\mathcal{B}) = \lim_{n \mapsto \infty} \mathcal{Q}^{(1)}(\mathcal{B}^{\otimes n})/n$ [21, 32–34]. There are stunning examples of channels which display non-additivity: for any integer $m > 1$ there is a channel $\tilde{\mathcal{B}}$ for which $\mathcal{Q}^{(1)}(\tilde{\mathcal{B}}^{\otimes m}) = 0$ but $\mathcal{Q}^{(1)}(\tilde{\mathcal{B}}^{\otimes k}) > 0$ for some $k > m$ [26]. Such unusual non-additivity implies that checking positivity of $\mathcal{Q}$ is hard.

Results.—Our *first* main contribution is to construct a simple noisy channel whose quantum and private capacity can be computed, but then show how a counter-intuitive scheme to allow leakage of almost all quantum information to the channel's environment boosts the channel's quantum and private capacities. This unexpected boost comes from leveraging non-additivity that has challenged our understanding of quantum capacities in the past. In the present case, non-additivity is used to show that strongly engaging a system with its environment increases the system's ability to protect entanglement and send private information.

Allowing leakage of information to a channel's environment is not expected to improve it's ability to send quantum information. This expectation is not entirely misplaced, indeed we find no increase in the channel's one-letter coherent information. However allowing leakage increases the coherent information over two uses of the channel. This key observation can be intuitively understood by constructing a special mixed input state which is entangled across two joint uses of the modified channel. Since the channel can heavily leaks quantum information, the input entanglement appears at the joint channel environment but does not appear at the joint channel output. The entangled environment state can be decomposed as a convex combination of two closely packed quantum states while the output state can be decomposed as a convex combination of two well separated states. These well separated states give more entropy to the output than closely packed states give to the environment. This difference in entropy boosts the coherent information. This boost implies that random codes in the typical subspace of this entangled input can send quantum information at larger rates than the original channel. Since this leakage based boost increases the two-letter coherent but not the one-letter coherent information, it gives rise to a sought after two-letter level non-additivity.

Despite its central importance, the general origin of non-additivity is obscure. In certain cases it is possible to transform a channel with additive coherent information into one with non-additive coherent information. One method, used to great effect in superactivation [35–37], is to place channels in parallel. Another method is to place channels in series [38, 39]. Clarifying when and how such methods work is a key challenge in quantum information. It is clear that placing channels in series decreases their capacity. While parallel use can non-additively increase the capacity, it also increases the channel's output dimension. A key finding in our work is that allowing leakage of information to a channel's environment is an entirely new way to obtain non-additivity. Unlike previous methods, this non-additivity increases a channel's quantum and private capacity without increasing the channel's output dimension. The amount of non-additivity found this way is an order of magnitude larger than found earlier.

Our leakage scheme introduces a gap between channel parameter values where $\mathcal{Q}^{(1)}$ is zero and where $\mathcal{Q}$ can be shown to vanish. To fill this gap, one must either show that $\mathcal{Q} = 0$ or show $\mathcal{Q} > 0$ for all parameters in the gap. Filling such gaps [40–44] is crucial to understanding a channel's quantum capacities. In most cases, including the well studied case of a qubit depolarizing channel, such gaps remain unfilled. However, we completely fill ours by showing $\mathcal{Q} > 0$ using an extremely clean argument based on a new insight into the von-Neumann entropy.

This insight, which is our *second* key contribution, is that logarithmic singularities (also called log-singularities) in the von-Neumann entropy S are a novel mechanism that gives rise to positive quantum capacity. The singularity occurs in the entropy of a density operator whose eigenvalues increase linearly from zero to leading order in some parameter ϵ of the density operator. As a result, for small values of ϵ the behaviour of the von-Neumann entropy $S(\epsilon)$ is completely dominated by the singularity, i.e. $dS(\epsilon)/d\epsilon \simeq -x \log \epsilon$ where $x > 0$ is called the rate or the strength of the singularity. This singularity shows up as a sharp increase in the entropy of a density operator as it linearly moves from the boundary of the set of quantum states to a point in the relative interior of the set.

The main idea that captures how log-singularities give rise to quantum capacity is as follows. Consider a channel input, whose output and environment state have equal entropy. Next perturb the input such that a log-singularity occurs at the output which is stronger than the log-singularity in the environment. This stronger singularity will dominate the behaviour of the coherent information, forcing it to become positive and thus giving rise to a strictly positive quantum capacity.

Not only are log-singularities useful in specific cases, they provide very general insights. For instance given a channel $\mathcal{B}$ with input, output, and environment dimensions d_a, d_b, and d_c respectively, one can prove that

Theorem. If $d_c < d_b$ and $\mathcal{B}$ maps some pure state to an output of rank d_c, then $\mathcal{Q}^{(1)}(\mathcal{B}) > 0$.

This Theorem applies to a large variety of cases, including the complement of experimentally relevant qubit Pauli channels [45] and generalized erasure channels [39]. It has a particularly elegant *corollary*: when $d_a > 1$ and $d_b > d_a(d_c - 1)$ then $\mathcal{Q}^{(1)}(\mathcal{B}) > 0$. This corollary is a one of a kind test for quantum capacity. Unlike other tests which either depend on the form of a channel or use numerics, this tests only uses the dimensions of a channel.

Log-singularities are also a source of non-additivity. This can be seen as follows. Consider two density operators, each of which optimizes the coherent information of a channel. Next, perturbed the product of these density operators to cause a singularity at the output entropy of the joint channel. This singularity will dominate the coherent information of the joint channel, making it rise above the sum of the coherent information of each channel. Using this idea, one can show a new instance of non-additivity where a qubit amplitude damping channel $\mathcal{B}$ with $\mathcal{Q}(\mathcal{B}) = 0$ boosts the coherent information of a qutrit channel $\mathcal{B}'$, i.e., strict inequality holds in (1).

From the point of view of quantum error correction, this is a remarkable result. It states that there are qubits on which we can't perform error correction directly, nonetheless using these qubits as parts of larger quantum circuits boosts rates for quantum error correction. It would be an extremely interesting future application to design and implement such quantum error correction schemes.

References

[1] Howard Wiseman. Death by experiment for local realism. *Nature*, 526(7575):649–650, Oct 2015. doi:10.1038/nature15631.

[2] J. S. Bell. On the einstein podolsky rosen paradox. *Physics Physique Fizika*, 1:195–200, Nov 1964. doi:10.1103/PhysicsPhysiqueFizika.1.195.

[3] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, Oct 1969. doi:10.1103/PhysRevLett.23.880.

[4] J. Maldacena and L. Susskind. Cool horizons for entangled black holes. *Fortschritte der Physik*, 61(9):781–811, 2013. doi:10.1002/prop.201300020.

[5] Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. Mip*=re, 2020. arXiv:2001.04383.

[6] Luigi Amico, Rosario Fazio, Andreas Osterloh, and Vlatko Vedral. Entanglement in many-body systems. *Rev. Mod. Phys.*, 80:517–576, May 2008. doi:10.1103/RevModPhys.80.517.

[7] Charles H. Bennett and Stephen J. Wiesner. Communication via one- and two-particle operators on einstein-podolsky-rosen states. *Phys. Rev. Lett.*, 69:2881–2884, Nov 1992. doi:10.1103/PhysRevLett.69.2881.

[8] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, Mar 1993. doi:10.1103/PhysRevLett.70.1895.

[9] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7 – 11, 2014. doi:10.1016/j.tcs.2014.05.025.

[10] Artur K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67:661–663, Aug 1991. doi:10.1103/PhysRevLett.67.661.

[11] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 74:145–195, Mar 2002. doi:10.1103/RevModPhys.74.145.

[12] Richard Cleve and Harry Buhrman. Substituting quantum entanglement for communication. *Phys. Rev. A*, 56:1201–1204, Aug 1997. doi:10.1103/PhysRevA.56.1201.

[13] Harry Buhrman, Richard Cleve, and Wim van Dam. Quantum entanglement and communication complexity. *SIAM Journal on Computing*, 30(6):1829–1841, 2001. doi:10.1137/S0097539797324886.

[14] Časlav Brukner, Marek Żukowski, Jian-Wei Pan, and Anton Zeilinger. Bell's inequalities and quantum communication complexity. *Phys. Rev. Lett.*, 92:127901, Mar 2004. doi:10.1103/PhysRevLett.92.127901.

[15] P. Kómár, E. M. Kessler, M. Bishof, L. Jiang, A. S. Sørensen, J. Ye, and M. D. Lukin. A quantum network of clocks. *Nature Physics*, 10(8):582–587, Aug 2014. doi:10.1038/nphys3000.

[16] N. Kalb, A. A. Reiserer, P. C. Humphreys, J. J. W. Bakermans, S. J. Kamerling, N. H. Nickerson, S. C. Benjamin, D. J. Twitchen, M. Markham, and R. Hanson. Entanglement distillation between solid-state quantum network nodes. *Science*, 356(6341):928–932, 2017. doi:10.1126/science.aan0070.

[17] I. V. Inlek, C. Crocker, M. Lichtman, K. Sosnova, and C. Monroe. Multispecies trapped-ion node for quantum networking. *Phys. Rev. Lett.*, 118:250502, Jun 2017. doi:10.1103/PhysRevLett.118.250502.

[18] Siddarth Koduru Joshi, Djeylan Aktas, Sören Wengerowsky, Martin Lončarić, Sebastian Philipp Neumann, Bo Liu, Thomas Scheidl, Guillermo Currás Lorenzo, Željko Samec, Laurent Kling, Alex Qiu, Mohsen Razavi, Mario Stipčević, John G. Rarity, and Rupert Ursin. A trusted node–free eight-user metropolitan quantum communication network. *Science Advances*, 6(36), 2020. doi:10.1126/sciadv.aba0959.

[19] H. J. Kimble. The quantum internet. *Nature*, 453(7198):1023–1030, Jun 2008. doi:10.1038/nature07127.

[20] John Preskill. Quantum Computing in the NISQ era and beyond. *Quantum*, 2:79, August 2018. doi:10.22331/q-2018-08-06-79.

[21] I. Devetak. The private classical capacity and quantum capacity of a quantum channel. *IEEE Transactions on Information Theory*, 51(1):44–55, Jan 2005. doi:10.1109/TIT.2004.839515.

[22] C. E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27(3):379–423, 1948. doi:10.1002/j.1538-7305.1948.tb01338.x.

[23] Howard Barnum, M. A. Nielsen, and Benjamin Schumacher. Information transmission through a noisy quantum channel. *Phys. Rev. A*, 57:4153–4175, Jun 1998. doi:10.1103/PhysRevA.57.4153.

[24] David P. DiVincenzo, Peter W. Shor, and John A. Smolin. Quantum-channel capacity of very noisy channels. *Phys. Rev. A*, 57:830–839, Feb 1998. doi:10.1103/PhysRevA.57.830.

[25] Ke Li, Andreas Winter, XuBo Zou, and GuangCan Guo. Private capacity of quantum channels is not additive. *Phys. Rev. Lett.*, 103:120501, Sep 2009. doi:10.1103/PhysRevLett.103.120501.

[26] Toby Cubitt, David Elkouss, William Matthews, Maris Ozols, David Pérez-García, and Sergii Strelchuk. Unbounded number of channel uses may be required to detect quantum capacity. *Nature Communications*, 6:6739, Mar 2015. doi:10.1038/ncomms7739.

[27] David Elkouss and Sergii Strelchuk. Superadditivity of private information for any number of uses of the channel. *Phys. Rev. Lett.*, 115:040501, Jul 2015. doi:10.1103/PhysRevLett.115.040501.

[28] Graeme Smith and John A. Smolin. Extensive nonadditivity of privacy. *Phys. Rev. Lett.*, 103:120503, Sep 2009. doi:10.1103/PhysRevLett.103.120503.

[29] Graeme Smith and John A. Smolin. Degenerate quantum codes for pauli channels. *Phys. Rev. Lett.*, 98:030501, Jan 2007. doi:10.1103/PhysRevLett.98.030501.

[30] Jesse Fern. Correctable noise of quantum-error-correcting codes under adaptive concatenation. *Phys. Rev. A*, 77:010301, Jan 2008. doi:10.1103/PhysRevA.77.010301.

[31] Graeme Smith, Joseph M. Renes, and John A. Smolin. Structured codes improve the bennett-brassard-84 quantum key rate. *Phys. Rev. Lett.*, 100:170502, Apr 2008. doi:10.1103/PhysRevLett.100.170502.

[32] Seth Lloyd. Capacity of the noisy quantum channel. *Phys. Rev. A*, 55:1613–1622, Mar 1997. doi:10.1103/PhysRevA.55.1613.

[33] Howard Barnum, E. Knill, and M. A. Nielsen. On quantum fidelities and channel capacities. *IEEE Trans. Info. Theor*, pages 1317–1329, 2000.

[34] Peter W. Shor. Quantum error correction, Nov 2002. `http://www.msri.org/workshops/203/schedules/1181`.

[35] Graeme Smith and Jon Yard. Quantum communication with zero-capacity channels. *Science*, 321(5897):1812–1815, 2008. doi:10.1126/science.1162242.

[36] Graeme Smith, John A. Smolin, and Jon Yard. Quantum communication with gaussian channels of zero quantum capacity. *Nature Photonics*, 5(10):624–627, Aug 2011. doi:10.1038/nphoton.2011.203.

[37] Fernando G. S. L. Brandão, Jonathan Oppenheim, and Sergii Strelchuk. When does noise increase the quantum capacity? *Phys. Rev. Lett.*, 108:040501, Jan 2012. doi:10.1103/PhysRevLett.108.040501.

[38] Felix Leditzky, Debbie Leung, and Graeme Smith. Dephrasure channel and superadditivity of coherent information. *Phys. Rev. Lett.*, 121:160501, Oct 2018. doi:10.1103/PhysRevLett.121.160501.

[39] Vikesh Siddhu and Robert B. Griffiths. Positivity and nonadditivity of quantum capacities using generalized erasure channels, Mar 2020. arXiv:2003.00583.

[40] Jesse Fern and K. Birgitta Whaley. Lower bounds on the nonzero capacity of pauli channels. *Phys. Rev. A*, 78:062335, Dec 2008. doi:10.1103/PhysRevA.78.062335.

[41] Felix Leditzky, Debbie Leung, and Graeme Smith. Quantum and private capacities of low-noise channels. *Phys. Rev. Lett.*, 120:160503, Apr 2018. doi:10.1103/PhysRevLett.120.160503.

[42] Sumeet Khatri, Kunal Sharma, and Mark M. Wilde. Information-theoretic aspects of the generalized amplitude-damping channel. *Phys. Rev. A*, 102:012401, Jul 2020. doi:10.1103/PhysRevA.102.012401.

[43] Johannes Bausch and Felix Leditzky. Quantum codes from neural networks. *New Journal of Physics*, 22(2):023005, Feb 2020. doi:10.1088/1367-2630/ab6cdd.

[44] Johannes Bausch and Felix Leditzky. Error thresholds for arbitrary pauli noise, Oct 2019. arXiv:1910.00471.

[45] Debbie Leung and John Watrous. On the complementary quantum capacity of the depolarizing channel. *Quantum*, 1:28, Sep 2017. doi:10.22331/q-2017-09-19-28.

[46] J. Eisert, M. Cramer, and M. B. Plenio. Colloquium: Area laws for the entanglement entropy. *Rev. Mod. Phys.*, 82:277–306, Feb 2010. doi:10.1103/RevModPhys.82.277.

[47] John Goold, Marcus Huber, Arnau Riera, Lídia del Rio, and Paul Skrzypczyk. The role of quantum information in thermodynamics—a topical review. *Journal of Physics A: Mathematical and Theoretical*, 49(14):143001, feb 2016. doi:10.1088/1751-8113/49/14/143001.