Research Statement

Sayantan Chakraborty
Tata Institute of Fundamental Research, Mumbai
sayantan.chakraborty@tifr.res.in, kingsbandz@gmail.com

April 2021

I am broadly interested in randomized algorithms, classical and quantum information theory and combinatorics. Currently I am working in two different areas, one of which stems from the study of entanglement transmission codes in quantum information theory and the other from the design and analysis of algorithms which sample *perfectly* (zero error in total variation) from some target distribution. Below, I give a brief overview of these topics and a brief overview of my recent work related to these topics.

1 Single Shot Entanglement Transmission Over Quantum Networks

In the past 70 years, few fields of research have had as ubiquitous and as profound an impact on both theory and practice as information and coding theory. Founded by Claude Shannon in his 1948 paper 'A Mathematical Theory of Communication', information theory provides the mathematical toolbox for us to answer the following questions:

- Given a noisy channel, what is the maximum rate at which information may be transmitted through it, so as to allow unique decoding with a small probability of error.
- Given a data file, what is the maximum rate of compression achievable so that the original file may be recovered from the compressed version with only a small loss.

Shannon provided the answer for both these questions and also showed the existence of encoding and decoding schemes which achieve the best possible bounds in both scenarios. Unfortunately, Shannon's constructions suffer from two main caveats:

- The codes Shannon designed are not *explicit* as in efficient encoding and decoding schemes are not known for them.
- They require an asymptotically infinite amount of resources (channel uses / samples from the source) to provide meaningful guarantees.

Recently, the situation described above has been generalized in two important ways :

- **Finite Blocklength and Single Shot Regime :** One considers the far more practically feasible setting when the amount of resources available are limited. For example, in the single shot regime, one is allowed only one use of the noisy channel.
- **Quantum Shannon Theory :** The theory of quantum mechanics offers a far richer set of tools than is available in the purely classical setting. It is only natural to consider whether one can perform information transmission, storage and retrieval tasks based on the rules of quantum mechanics. Indeed, it is known that using quantum mechanical tools we are able to perform certain information processing tasks which are impossible in the classical world (superactivation of Holevo capacity [1], information locking [2]), etc.

I am interested in showing the existence of efficient coding and decoding techniques in this general framework, when there are multiple parties (both senders and receivers) taking part in the protocol. To be specific, I am interested in showing the existence of efficient *entanglement transmission codes* for general multi terminal channels. Entanglement transmission is the task where the sender holds one half of an Einstein-Podolosky-Rosen (EPR) pair and sends one half of it through a noisy channel. The protocol requires the receiver to be able to recover the transmitted half with a small amount of error. At the end of the protocol, the sender and receiver manage to share entanglement.

This task has major real world applications, including Quantum Key Distribution (QKD) and secret communication which is secure against quantum attacks, to name a few.

While this problem has been studied extensively, both in the asymptotic iid and the single shot settings [3, 4, 5] for the case of a single sender and a single receiver, very little is known for the case when multiple parties are involved.

In this context, I would like to mention some recent results which I co-authored with my advisor Prof. Pranab Sen and colleague Aditya Nema :

In the paper [6] we studied entanglement transmission over the multiple access channel (two senders one receiver), when only *one* use of the channel is available. Prior to our work, entanglement transmission codes were known to exist for this channel when asymptotically many copies of the channel were available. We established that entanglement can be transmitted independently by the two senders to the receiver, even when only a single use of the channel is allowed. Along the way, we generalized several foundational coding techniques to the fully quantum regime that previously were only known in the classical regime such as rate splitting and successive cancellation. Our techniques recover the best known bounds when asymptotically many uses of the channel are available for any amount of pre-shared entanglement. In addition, the techniques in that paper seem to give the first non-trivial bounds for entanglement transmission over the quantum interference channel, which has two senders and two receivers. The task is for sender 1 to transmit entanglement to receiver 1 and the same for sender 2 and receiver 2. Previously, aside from trivial bounds, nothing was known for entanglement transmission over this channel, even in the asymptotic iid setting. An older version of this paper was accepted as a contributed talk at the Beyond IID 8, 2020 [7]. The current version will appear in the proceedings of ISIT 2021.

In the paper [8] we asked whether there exists a *multi sender decoupling theorem*. Decoupling theorems [9] are essential to multiple quantum protocols, including state merging [10], random subspace measurements, etc. However, previously only a single sender single receiver version of the theorem was known in the literature. We showed the existence of multi sender version of the decoupling theorem, which directly implies the existence of simultaneous decoders for many multi terminal channels. Modulo a simultaneous smoothing conjecture (which remains open), this would imply the best known results for entanglement transmission, even in the asymptotic iid setting. The results in this work will appear in the proceedings of ISIT 2021.

A natural question that arises in connection to the techniques used in the works mentioned above is whether they can be used to send classical information over a quantum multiple access channel in the presence of an eavesdropper. Formally, the two senders want to send classical messages to the receiver independently, such that:

- Reliability : The receiver is able to decode each sender's message with a high probability of success.
- Secrecy : The eavesdropper cannot distinguish among the message pairs that are transmitted through the channel by the two senders.

This problem is potentially harder than the problem of sharing EPR pairs via the quantum MAC, simply because the protocol should be able to guarantee secrecy against an arbitrary type of eavesdropper, and not only when the eavesdropper is the *purifying environment*, which is the only kind of eavesdropper we need to consider while designing entanglement transmission codes. Note also that this problem is a natural generalisation of the point to point wiretap channel to the multiterminal setting.

In the paper [11] we give the first non-trivial bounds known for this problem in the one shot setting. The main bottleneck in proving such a result is that one has to prove a distributed covering lemma, which is the heart of the secrecy part of the protocol. We note that a version of this lemma was known in the folklore for some time. But this version is unsatisfactory since it requires a simultaneous smoothing conjecture to give the best bounds in both the one shot and asymptotic iid setting. We instead proved a novel variation of this distributed covering lemma, which we informally refer to as a 'successive cancellation style covering lemma', which allowed us to generalise our bounds to the asymptotic iid setting without appealing to the smoothing conjecture. This work is currently under submission at ITW 2021.

1.1 Future Research Focus

In the works mentioned till now we have been able to make progress towards a theory of information transmission over multi terminal channels, with very few available resources. However, the encoding and decoding schemes we have proposed still rely on a randomization argument. I will now focus my efforts towards making these constructions *efficient*. Recently, efficient encoder constructions have been shown for the single sender single receiver case based

on Arikan's polar coding techniques [12]. An important caveat however is that efficient decoding is still unknown. Furthermore, the polarisation phenomenon, which is at the heart of showing the existence of efficient encoders and decoders in the classical regime are not well understood in the fully quantum regime. I will try to design a fully quantum efficient encoding decoding scheme for entanglement transmission, by leveraging the polarisation phenomenon. This in turn will imply efficient coding strategies for most multi terminal scenarios, bridging the gap between theory and practice.

2 Perfect Sampling Algorithms

In this section we will change tracks from information and coding theory to the study of sampling algorithms, in particular perfect sampling algorithms. Broadly, sampling algorithms are designed to sample from a distribution supported on some combinatorial structure such as k-colorings or the independent sets of a graph, either approximately or perfectly (with zero error), in polynomial time.

As mentioned earlier, a perfect sampling algorithm samples from target distribution with zero error in total variation. A specific example of a perfect sampling problem is as follows : We are given a graph G with number of vertices n and max degree Δ. We are also given k colors. The problem is to produce a uniformly random proper coloring from the set of all proper k colorings of G.

Another variant of a sampling problem is the problem of sampling from the hard core model: Given a graph G with max degree Δ and size n, and also given a parameter λ known as the fugacity, produce a sample from the following distribution which is supported on the independent sets $\mathcal{I} \subset V$ of the graph:

$$\mathcal{I} \sim \frac{\lambda^{|\mathcal{I}|}}{\sum_{\mathcal{I}} \lambda^{|\mathcal{I}|}}$$

For the problem of sampling colorings, Jerrum showed that as long as $k > 2\Delta$, there exists an algorithm which can sample from a distribution ϵ close in total variation to the uniform distribution on proper colorings, in time polynomial in n. This variant of the sampling problem is referred to as approximate sampling, and has enjoyed a great deal of attention from the sampling community.

However, I am interested in perfect sampling, since, for example, there might be situations where a *perfect* random bit is necessary and an *almost* random bit, not matter how close to totally uniform, may not do the job. That perfect sampling can be done at all is an amazing fact, have been shown for the first time by Propp and Wilson [13] in their seminal paper. Subsequently, Huber[14] showed that there exists a perfect sampling algorithm for k-colorings as long as $k > O(\Delta^2)$. He also showed analogous bounds for the hard core model.

In this context I would like to describe a recent paper I authored with my colleague Siddharth Bhandari (TIFR). In that paper [15], we showed that there exists a perfect sampling algorithm which produces a uniformly random proper k-coloring of the given graph in polynomial time, as long as $k > 3\Delta$. This answered a long standing question of whether the quadratic dependence on the max degree for the number of colors necessary to produce a uniformly random coloring could be brought down to linear. This paper won the *Danny Lewin Best Student Paper Award* at STOC 2020.

It is well known that it is hard to sample from the hard core distribution, when $\lambda \gtrsim \frac{e}{\Delta}$ unless `NP=RP` [16]. Recently it has been shown that Markov Chain Monte Carlo based algorithms can sample efficiently and approximately right up to this critical value [17]. A similar result is not known for perfect sampling.

I along with my collaborators Siddharth Bhandari and Piyush Srivastava have been able to answer this question for perfect sampling, albeit for a subclass of graphs with large ($> O(\log n)$) degree. Our results also require some assumptions on the girth of the graph, although our assumptions do not require the girth to be a function of the size of the graph. The manuscript of this result is under preparation.

2.1 Future Research Focus

I am broadly interested in the following question :

A broader goal is to show a theorem of the sort 'approximate sampling algorithms which use Markov Chain Monte Carlo imply perfect sampling'. A long term goal of mine is to prove a theorem of this sort such that we can show

the equivalence of MCMC methods and perfect sampling. Even a negation of this will give us important insight into combinatorial structures and show separations between approximate and perfect sampling.

3 Conclusion

In summary, I am interested in designing efficient protocols for sending entanglement across different quantum networks with a small amount of error. I have already shown the existence of protocols which achieve this goal across various multi user quantum channels. I plan to work towards making these protocols efficient for use in real world scenarios. I am also interested in perfect sampling algorithms. I have already provided an algorithm which produces a uniformly random k-coloring for a bounded degree graph in poly time, given only linearly many colors. This result closes the gap between perfect and approximate sampling of k-colorings which had persisted for some time. I am now working towards showing the existence of an efficient algorithm which perfectly samples an independent set from the hard core distribution, with a fugacity which is slightly smaller than the critical value.

References

[1] M. B. Hastings. Superadditivity of communication capacity using entangled inputs. *Nature Physics*, 5(4):255–257, Apr 2009. ISSN 1745-2481. doi: 10.1038/nphys1224. URL https://doi.org/10.1038/nphys1224.

[2] Omar Fawzi, Patrick Hayden, and Pranab Sen. From low-distortion norm embeddings to explicit uncertainty relations and efficient information locking. *J. ACM*, 60(6), November 2013. ISSN 0004-5411. doi: 10.1145/2518131. URL https://doi.org/10.1145/2518131.

[3] I. Devetak. The private classical capacity and quantum capacity of a quantum channel. *IEEE Transactions on Information Theory*, 51(1):44–55, 2005.

[4] Patrick Hayden, Michal Horodecki, Jon Yard, and Andreas Winter. A decoupling approach to the quantum capacity. *Open Systems Information Dynamics*, 15, 03 2007. doi: 10.1142/S1230161208000043.

[5] F. Buscemi and N. Datta. The quantum capacity of channels with arbitrarily correlated noise. *IEEE Transactions on Information Theory*, 56(3):1447–1460, 2010.

[6] Sayantan Chakraborty, Aditya Nema, and Pranab Sen. Novel one-shot inner bounds for unassisted fully quantum channels via rate splitting. Available at arXiv:2102.01766, 2021.

[7] Sayantan Chakraborty. One-shot inner bounds for the unassisted quantum multiple access channel via simultaneous decoding and rate splitting. *Contributed talk, Beyond IID 8*, 2020. Recorded Video.

[8] Sayantan Chakraborty, Aditya Nema, and Pranab Sen. A multi sender decoupling theorem and simultaneous decoding for the quantum mac. Available at arXiv:2102.02187, 2021.

[9] Frédéric Dupuis. The decoupling approach to quantum information theory. 04 2010.

[10] Michał Horodecki, Jonathan Oppenheim, and Andreas Winter. Quantum state merging and negative information. *Communications in Mathematical Physics*, 269(1):107–136, Jan 2007. ISSN 1432-0916. doi: 10.1007/s00220-006-0118-x. URL https://doi.org/10.1007/s00220-006-0118-x.

[11] Sayantan Chakraborty, Aditya Nema, and Pranab Sen. One-shot inner bounds for sending private classical information over a quantum MAC. *arXiv e-prints*, art. arXiv:2105.06100, May 2021.

[12] E. Arikan. Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels. *IEEE Transactions on Information Theory*, 55(7):3051–3073, 2009. doi: 10.1109/TIT.2009.2021379.

[13] James Gary Propp and David Bruce Wilson. Exact sampling with coupled Markov chains and applications to statistical mechanics. *Random Structures Algorithms*, 9(1-2):223–252, 1996. URL https://doi.org/10.1002/(SICI)1098-2418(199608/09)9:1/2<223::AID-RSA14>3.0.CO;2-O.

[14] M. Huber. Exact sampling and approximate counting techniques. In *Proceedings of the Thirtieth Annual ACM Symposium on the Theory of Computing, Dallas, Texas, USA, May 23-26, 1998*, pages 31–40, 1998. doi: 10.1145/276698.276709. URL https://doi.org/10.1145/276698.276709.

[15] Siddharth Bhandari and Sayantan Chakraborty. Improved bounds for perfect sampling of k-colorings in graphs. In *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2020, page 631–642, New York, NY, USA, 2020. Association for Computing Machinery. ISBN 9781450369794. doi: 10.1145/3357713.3384244. URL https://doi.org/10.1145/3357713.3384244.

[16] A. Sly. Computational transition at the uniqueness threshold. In *2010 IEEE 51st Annual Symposium on Foundations of Computer Science*, pages 287–296, 2010. doi: 10.1109/FOCS.2010.34.

[17] Z. Chen, K. Liu, and E. Vigoda. Rapid mixing of glauber dynamics up to uniqueness via contraction. In *2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1307–1318, 2020. doi: 10.1109/FOCS46700.2020.00124.