PCP Reading

July 17, 2020

1 Introduction

Roughly speaking, Probabilistically Checkable Proofs (PCPs) embody the study of "robust" computation. More specifically, the classical PCP theorem gives a new "robust" interpretation to proof verification in NP. It establishes that any NP proof can be carefully rewritten in a robust way (with at most a polynomial size blow-up) such that for a probabilistic verifier it is enough to query only a constant number of bits in this new robust proof to decide, with constant probability, the validity of a statement. To implement this robustness, error correcting codes with certain local properties and also expander graphs turned out to be very fruitful objects. From its very local view of the proof (randomly chosen), the verifier has to deduce the correctness of a given statement. This gives rise to the study of local-to-global phenomena embodied in so-called agreement tests.

Brute forcing over all possible local views a verifier can generate during its execution gives rise to a constraint satisfaction problem (CSP). Thus, it is not hard to see that a PCP readily implies hardness of approximation for CSPs (with constraints given by the verifier's acceptance rules). In fact, the development of tailored PCP theorems helped clarify large portions of the intricate landscape of hardness of approximation [Hås01]. However, the hardness of approximation of many fundamental problems is still open. A noteworthy example being our beloved MaxCut which is arguably one of the simplest kind of Max-CSPs. To patch our knowledge gap, a seemingly restricted PCP known as Unique Games (UG) was proposed by Khot [Kho10]. Thanks to its more restricted nature, it made UG handy in hardness reductions. Soon many unknown hardness of approximation results were tied to UG-hardness. Therefore, the conjecture that UG is NP-hard to approximate became an important open problem and its resolution has enjoyed great progress over the years (with "evidence" going in both directions).

Another application of PCPs going beyond its initial [1] role in hardness of approximation is the delegation/verification of computation. In this setting one might want to allow interactions between a prorver and a verifier. If you submit a computational task to a powerful cloud ("the prover"), you ("the verifier") might want to check the computation was correctly performed without having to recompute it yourself. A possible scenario is the following, we might want assume that the cloud can perform arbitrary polynomial time computation (rather than having NP powers) and the verifier is even more restricted but is allowed to ask questions to the cloud. This line of research has enjoyed great progress and we have compelling reasons to make the PCP technology practically viable. See the monograph on doubly-efficient interactive proof systems of Goldreich [Gol18].

[1] Strictly speaking interactive proof systems (which is a form of delegation of computation) came historically first, but the initial bulk of applications came form the connection of PCP with hardness of approximation.

Yet another fascinating direction of the PCP study emerged with the quantum computational model. The CSP version of the quantum PCP conjecture is widely open and it seems to require fundamentally new ideas.

2 Classical PCP

The proof of the PCP theorem comes in two main flavors: algebraic and combinatorial. They appear in the following seminal works.

- In [ALM+98], Arora et al. use error correcting codes and composition to prove the PCP theorem.
- In [Din06], Dinur use exapnders in an iterative procedure to amplify the gap of a CSP ("spread the jam") until it becomes constant.

A precursor of the PCP theorem for NP was a the equivalence of MIP = NEXP by Babai et al. [BFL90]. It has motivating the scaling down race towards the PCP theorem for NP and it has also influence the quantum development of NEXP $\subseteq$ MIP* by Ito–Vidick [IV12].

2.1 Low Degree Test

Given a function purported to be the evaluation of low degree polynomial, how can we locally certify this?

- In[Sud92], Sudan give an account of low degree tests.
- In [Gol17, Chapter 3], Goldreich presents low degree tests.

2.2 Interactive Oracle Proofs

An important open question in the PCP literature is whether PCPs of linear length can be constructed. If one allows interaction in a model called Interactive Oracle Proofs (IOP), then Ben-Sasson et al. [BCG+17] show that this is indeed possible. More recently, Ron-Zewi and Rothblum showed the size blow-up constant can be made arbitrarily close to 1.

2.3 Derandomization

In [AB19], Aharonov and Grilo show that a PCP for MA (suitably defined) would imply MA=NP.

3 Unique Games

The Unique Games Conjecture asserts that for every $\epsilon > 0$ there exists a sufficiently large alphabet size $q \in \mathbb{N}$ such that distinguishing whether a 2-CSP with permutation constraints on alphabet $[q]$ is at least $1 - \epsilon$ satisfiable or at most ϵ satisfiable is NP-hard.

- In [DKK+18a, DKK+18b], Dinur et al. describe an efficient reduction from gap-3LIN to 2-to-1 games and explore non-expanding structures of the Grassmann graph to study its hardness. Combined with Barak et al. [BKS19], this gives a full proof of the 2-to-1 Conjecture.

4 Quantum PCP

In the classical setting, the proof verfication, CSP and multiprover versions of PCPs are equivalent. However, in the quantum setting this is no longer true. The multiprover version with entangled provers turned out to be surprisingly more powerful this was shown in a sequence of results that culminated in the impressive MIP* = RE result by Ji et al. [JNV$^+$20]. Fortunately, the quantum "CSP" version known as Quantum local-Halmitonian PCP is still a widely open conjecture. Its resolution might involve better understanding of quantum codes/states.

- An older survey of the quantum PCP Conjecture by Aharonov et al. [AAV13] (some breakthroughs afterwards).
- In [AALV09], Aharonov et al. introduce the detectability lemma to analyze the structure of frustation free Hamiltonians (analog CSPs with perfect completeness) and design a Dinur style gap amplification procedure. See Anshu et al. [AAV16] for a simplified proof.
- In [EKZ20], Evra et al. use HDXs to design LDPC quantum codes beyond $\sqrt{n}$ distance. One can ask if their ideas have any PCP application.

References

[AALV09] Dorit Aharonov, Itai Arad, Zeph Landau, and Umesh Vazirani. The detectability lemma and quantum gap amplification. In *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing*, STOC 09, page 417426, 2009.

[AAV13] Dorit Aharonov, Itai Arad, and Thomas Vidick. The quantum pcp conjecture, 2013.

[AAV16] Anurag Anshu, Itai Arad, and Thomas Vidick. Simple proof of the detectability lemma and spectral gap amplification. *Physical Review B*, 93(20), May 2016.

[AB19] D. Aharonov and A. Bredariol Grilo. Stoquastic pcp vs. randomness. In *2019 IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1000–1023, 2019.

[ALM$^+$98] Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, and Mario Szegedy. Proof verification and the hardness of approximation problems. *J. ACM*, 45(3):501555, May 1998.

[BCG$^+$17] Eli Ben-Sasson, Alessandro Chiesa, Ariel Gabizon, Michael Riabzev, and Nicholas Spooner. Interactive oracle proofs with constant rate and query complexity. In Ioannis Chatzigiannakis, Piotr Indyk, Fabian Kuhn, and Anca Muscholl, editors, *44th International Colloquium on Automata, Languages, and Programming, ICALP 2017, July 10-14, 2017, Warsaw, Poland*, volume 80 of *LIPIcs*, pages 40:1–40:15, 2017.

[BFL90] L. Babai, L. Fortnow, and C. Lund. Nondeterministic exponential time has two-prover interactive protocols. In *Proceedings [1990] 31st Annual Symposium on Foundations of Computer Science*, pages 16–25 vol.1, 1990.

[BKS19] Boaz Barak, Pravesh K. Kothari, and David Steurer. Small-set expansion in shortcode graph and the 2-to-2 conjecture. In *10th Innovations in Theoretical Computer Science Conference, ITCS 2019, January 10-12, 2019, San Diego, California, USA*, pages 9:1–9:12, 2019.

[Din06] Irit Dinur. The PCP theorem by gap amplification. In *Proc. 38th ACM Symp. on Theory of Computing*, pages 241–250, 2006.

[DKK+18a] Irit Dinur, Subhash Khot, Guy Kindler, Dor Minzer, and Muli Safra. On non-optimally expanding sets in grassmann graphs. In *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2018, page 940951, 2018.

[DKK+18b] Irit Dinur, Subhash Khot, Guy Kindler, Dor Minzer, and Muli Safra. Towards a proof of the 2-to-1 games conjecture? In *Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2018, page 376389, 2018.

[EKZ20] Shai Evra, Tali Kaufman, and Gilles Zmor. Decodable quantum ldpc codes beyond the $\sqrt{n}$ distance barrier using high dimensional expanders, 2020.

[Gol17] Oded Goldreich. *Low-Degree Tests*, page 4968. Cambridge University Press, 2017.

[Gol18] Oded Goldreich. On doubly-efficient interactive proof systems. *Foundations and Trends in Theoretical Computer Science*, 13(3):158–246, 2018.

[Hås01] Johan Håstad. Some optimal inapproximability results. *Journal of the ACM*, 48(4):798–859, 2001.

[IV12] Tsuyoshi Ito and Thomas Vidick. A multi-prover interactive proof for nexp sound against entangled provers. In *Proceedings of the 2012 IEEE 53rd Annual Symposium on Foundations of Computer Science*, FOCS 12, page 243252, 2012.

[JNV+20] Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. MIP*=RE, 2020.

[Kho10] Subhash Khot. Inapproximability of np-complete problems, discrete Fourier analysis, and geometry. In *Proceedings of the International Congress of Mathematicians*, 2010.

[Sud92] Madhu Sudan. *Efficient Checking of Polynomials and Proofs and the Hardness of Approximation Problems*. PhD thesis, USA, 1992.