

My main research area is computational complexity, which is the study of the reach of efficient computation. Here I have made several fundamental contributions. I have also developed connections with mathematics and finance, influencing leading researchers in both disciplines. In this page I provide a sample of the research I have done with my coauthors.

We have worked extensively on pseudorandom generators, which are efficient, deterministic procedures that stretch a short seed into a longer sequence that “looks random.” These fascinating objects are key to our understanding of the power of randomness in computation. For the model of polynomials, our generator [BV10, Vio09d] was the first progress after 15 years, and spurred interaction with mathematicians which led to progress [GT09] on a famous conjecture in mathematics. An exciting aspect of this generator, and one which I intend to explore, is that its power is still unknown: the generator is a candidate for solving other long-standing problems in pseudorandomness. More recently, we constructed the first generator for halfspaces [DGJ⁺10], obtaining along the way a result of independent interest in probability theory: the central limit theorem continues to hold for random variables that only enjoy limited independence. Our above works have been applied and extended widely [MZ09, LRTV09, SLS10, GKS10, DKN10, MZ10, GOWZ10]. For two single-authored papers on generators I received the 2006 SIAM Student Paper Prize [Vio07a] and, at the 2008 Computational Complexity Conference, the Best Paper Award [Vio09d].

We have also worked in communication complexity, which is the study of the amount of communication that players need to exchange to solve a problem. Here we focused on the challenging and useful number-on-forehead model, where players' inputs overlap. We obtained a state-of-the-art separation for the analogue of the P vs. NP question in this model [DPV09], and a lower bound for following a path in a graph [VW09] which solves a decade-old problem.

Succinct data structures is another area we worked on. Here the goal is one that is crucial to any computer system needing fast access to large data sets: store data using little redundancy while allowing for fast retrieval. We proved first and tight lower bounds for central problems such as storing non-binary arrays, sets, and trees [Vio, PV10].

Most recently, we have been working on a shift of paradigm in complexity. Rather than focusing on the complexity of solving a problem instance, the idea is to study the complexity of generating a random instance together with its solution. We have obtained several first-of-their-kind results and also revisited problems in pseudorandomness and data structures under this new angle [Vio10, LV10]. I plan to tackle the many problems left open by our works, which point to an uncharted and possibly fertile research area.

I am also dedicated to expository writing. I wrote two invited surveys [Vio09a, Vio09c], the latter containing unpublished material from a “Gems” class I developed [Vio09b]. A third survey [Vio07b] makes advanced results in combinatorics accessible to non-experts. I also collaborated to a popular-science book on finance [LH10], especially by writing a section on randomness from a computational point of view, thus promoting the ideas of theoretical computer science to a wider audience. I am in fact interested in connecting further finance and computer science. For example, through a videogame we gathered evidence [HLV10] that humans can tell price data from random. This refutes a folk belief, and raises the exciting possibility of harnessing human skills for price prediction through computer systems.

References

- [BV10] Andrej Bogdanov and Emanuele Viola. Pseudorandom bits for polynomials. *SIAM Journal on Computing*, 39(6):2464–2486, 2010. FOCS special issue.
- [DGJ⁺10] Ilias Diakonikolas, Parikshit Gopalan, Ragesh Jaiswal, Rocco A. Servedio, and Emanuele Viola. Bounded independence fools halfspaces. *SIAM Journal on Computing*, 39(8):3441–3462, 2010.
- [DKN10] Ilias Diakonikolas, Daniel Kane, and Jelani Nelson. Bounded independence fools degree-2 threshold functions. In *51th Symposium on Foundations of Computer Science (FOCS)*. IEEE, 2010.
- [DPV09] Matei David, Toniann Pitassi, and Emanuele Viola. Improved separations between nondeterministic and randomized multiparty communication. *ACM Trans. Comput. Theory*, 1(2):1–20, 2009.
- [GKS10] Parikshit Gopalan, Subhash Khot, and Rishi Saket. Hardness of reconstructing multivariate polynomials over finite fields. *SIAM J. Comput.*, 39(6):2598–2621, 2010.
- [GOWZ10] Parikshit Gopalan, Ryan O’Donnell, Y. Wu, and David Zuckerman. Fooling functions of halfspaces under product distributions. In *25th Annual Conference on Computational Complexity (CCC)*, 2010.
- [GT09] Ben Green and Terence Tao. The distribution of polynomials over finite fields, with applications to the Gowers norms. *Contrib. Discrete Math.*, 4(2):1–36, 2009.
- [HLV10] Jasmina Hasanhodzic, Andrew Lo, and Emanuele Viola. Is it real, or is it randomized?: A financial turing test, 2010. Available at SSRN: <http://ssrn.com/abstract=1558149>.
- [LH10] Andrew Lo and Jasmina Hasanhodzic. *The Evolution of Technical Analysis: Financial Prediction from Babylonian Tablets to Bloomberg Terminals*. Wiley, 2010.
- [LRTV09] Shachar Lovett, Omer Reingold, Luca Trevisan, and Salil P. Vadhan. Pseudo-random bit generators that fool modular sums. In *13th International Workshop on Randomization and Computation (RANDOM)*, volume 5687 of *Lecture Notes in Computer Science*, pages 615–630. Springer, 2009.
- [LV10] Shachar Lovett and Emanuele Viola. Bounded-depth circuits cannot sample good codes. Manuscript available at <http://www.ccs.neu.edu/home/viola>, 2010.
- [MZ09] Raghu Meka and David Zuckerman. Small-bias spaces for group products. In *13th International Workshop on Randomization and Computation (RANDOM)*, volume 5687 of *Lecture Notes in Computer Science*, pages 658–672. Springer, 2009.

- [MZ10] Raghu Meka and David Zuckerman. Pseudorandom generators for polynomial threshold functions. In *42nd ACM Symposium on Theory of Computing (STOC)*, pages 427–436. ACM, 2010.
- [PV10] Mihai Pătraşcu and Emanuele Viola. Cell-probe lower bounds for succinct partial sums. In *21th Symposium on Discrete Algorithms (SODA)*. ACM-SIAM, 2010.
- [SLS10] Partha Mukhopadhyay Shachar Lovett and Amir Shpilka. Pseudorandom generators for $CC^0[p]$ and the Fourier spectrum of low-degree polynomials over finite fields. In *51th Symposium on Foundations of Computer Science (FOCS)*. IEEE, 2010.
- [Vio] Emanuele Viola. Bit-probe lower bounds for succinct data structures. To appear in *SIAM Journal on Computing*, STOC special issue.
- [Vio07a] Emanuele Viola. Pseudorandom bits for constant-depth circuits with few arbitrary symmetric gates. *SIAM Journal on Computing*, 36(5):1387–1403, 2007.
- [Vio07b] Emanuele Viola. Selected results in additive combinatorics: An exposition. *Electronic Colloquium on Computational Complexity*, Technical Report TR07-103, 2007. www.eccc.uni-trier.de/.
- [Vio09a] Emanuele Viola. Correlation bounds for polynomials over $\{0, 1\}$. *SIGACT News, Complexity Theory Column*, 40(1), March 2009.
- [Vio09b] Emanuele Viola. Gems of theoretical computer science, 2009. Lecture notes of the class taught at Northeastern University. Available at <http://www.ccs.neu.edu/home/viola/classes/gems-08/index.html>.
- [Vio09c] Emanuele Viola. On the power of small-depth computation. *Foundations and Trends in Theoretical Computer Science*, 5(1):1–72, 2009.
- [Vio09d] Emanuele Viola. The sum of d small-bias generators fools polynomials of degree d . *Computational Complexity*, 18(2):209–217, 2009. CCC special issue.
- [Vio10] Emanuele Viola. The complexity of distributions. In *51th Symposium on Foundations of Computer Science (FOCS)*. IEEE, 2010.
- [VW09] Emanuele Viola and Avi Wigderson. One-way multiparty communication lower bound for pointer jumping with applications. *Combinatorica*, 29(6):719–743, 2009.