

# EMANUELE VIOLA

December 23, 2011

Northeastern University, 246 West Village H (WV), 440 Huntington Avenue, Boston, MA 02115  
Web: [www.ccs.neu.edu/home/viola](http://www.ccs.neu.edu/home/viola) Email: [viola@ccs.neu.edu](mailto:viola@ccs.neu.edu) Phone: (617) 373-8298

## RESEARCH INTERESTS

Computational complexity theory, pseudorandomness, cryptography, finance

## CURRENT POSITION

**Northeastern University**, Boston, MA Fall 2008 – present  
Assistant professor

## RESEARCH POSITIONS

**Columbia University**, New York, NY Fall 2007 – Summer 2008  
Postdoctoral fellow; Sponsor: Rocco Servedio

**Institute for Advanced Study**, Princeton, NJ Fall 2006 – Summer 2007  
Postdoctoral fellow; Sponsor: Avi Wigderson

## EDUCATION

**Harvard University**, Cambridge, MA Fall 2001 – Summer 2006  
Ph.D. Computer Science; Advisor: Salil Vadhan

**La Sapienza University**, Rome, Italy Fall 1995 – Spring 2000  
B.S. Computer Science, *summa cum laude*

## AWARDS

**NSF CAREER Award**, 0845003 2009

**Best Paper Award**, IEEE Conf. on Computational Complexity, for the paper [13] 2008

**SIAM Student Paper Prize**, for the paper [7] 2006

## PROFESSIONAL SERVICE

**Program committee**

16th Int. Workshop on Randomization and Computation RANDOM 2012

25th IEEE Conference on Computational Complexity CCC 2010

13th Int. Workshop on Randomization and Computation RANDOM 2009

49th IEEE Symp. on Foundations of Computer Science FOCS 2008

11th Int. Workshop on Randomization and Computation RANDOM 2007

**Grant reviewing**, NSF (panelist) 2008, 2009, 2011; Israel Science Foundation, 2009, 2010

## PREPRINTS

5. The communication complexity of addition  
Manuscript, 2011
4. Tight bounds on computing error-correcting codes by bounded-depth circuits with arbitrary gates  
With Anna Gál and Kristoffer Arnsfelt Hansen and Michal Koucký and Pavel Pudlák  
Manuscript, 2011
3. Block ciphers, pseudorandom functions, and natural proofs  
With Eric Miles  
Manuscript, 2011
2. Do humans perceive temporal order in asset returns?  
With Jasmina Hasanhodzic and Andrew Lo  
Manuscript, 2010
1. In Brute-Force Search of Correlation Bounds for Polynomials  
With Frederic Green and Daniel Kreymer  
Manuscript, 2011

## RESEARCH PAPERS

All of the conferences (and journals) below are peer reviewed.

24. Extractors for circuit sources  
In IEEE Symp. on Foundations of Computer Science (FOCS), 2011  
Invited and submitted to **FOCS Special Issue**
23. On beating the hybrid argument  
With Bill Fefferman and Ronen Shaltiel and Christopher Umans  
In ACM Innovations in Theoretical Computer Science conf. (ITCS), 2012
22. Randomness buys depth for approximate counting  
In IEEE Symp. on Foundations of Computer Science (FOCS), 2011
21. On the Complexity of Non-adaptively Increasing the Stretch of Pseudorandom Generators  
With Eric Miles  
In Theory of Cryptography Conf. (TCC), 2011
20. A Computational View of Market Efficiency  
With Jasmina Hasanhodzic and Andrew W. Lo  
Quantitative Finance, vol. 11, num. 7, 2011
19. Bounded-depth circuits cannot sample good codes  
With Shachar Lovett  
In IEEE Conf. on Computational Complexity (CCC), 2011  
Invited and submitted to special issue of Computational Complexity

18. The complexity of distributions  
To appear in *SIAM J. on Computing*  
Preliminary version in 51th IEEE Symp. on Foundations of Computer Science (FOCS), 2010
17. Cell-probe lower bounds for succinct partial sums  
With Mihai Pătraşcu  
In 21th ACM-SIAM Symp. on Discrete Algorithms (SODA), 2010
16. Bounded Independence Fools Halfspaces  
With Ilias Diakonikolas and Parikshit Gopalan and Ragesh Jaiswal and Rocco A. Servedio  
*SIAM J. on Computing*, vol. 39, num. 8, pp. 3441-3462, 2010  
Preliminary version in 50th IEEE Symp. on Foundations of Computer Science (FOCS), 2009
15. Bit-probe lower bounds for succinct data structures  
To appear in *SIAM J. on Computing*  
Preliminary version in 41th ACM Symp. on the Theory of Computing (STOC), 2009  
**STOC Special Issue**
14. Improved separations between nondeterministic and randomized multiparty communication  
With Matei David and Toniann Pitassi  
*ACM Trans. Computation Theory*, vol. 1, num. 2, pp. 1–20, 2009  
Preliminary version in 12th Workshop on Randomization and Computation (RANDOM), 2008
13. The sum of  $d$  small-bias generators fools polynomials of degree  $d$   
*Computational Complexity*, vol. 18, num. 2, pp. 209-217, 2009  
Preliminary version in IEEE Conf. on Computational Complexity (CCC), 2008  
**Best paper award**
12. Hardness amplification proofs require majority  
With Ronen Shaltiel  
*SIAM J. on Computing*, vol. 39, num. 7, pp. 3122-3154, 2010  
Preliminary version in 40th ACM Symp. on the Theory of Computing (STOC), 2008
11. One-way multiparty communication lower bound for pointer jumping with applications  
With Avi Wigderson  
*Combinatorica*, vol. 29, num. 6, pp. 719-743, 2009  
Preliminary version in 48th IEEE Symp. on Foundations of Computer Science (FOCS), 2007  
Invited to **FOCS Special Issue**
10. Pseudorandom bits for polynomials  
With Andrej Bogdanov  
*SIAM J. on Computing*, vol. 39, num. 6, pp. 2464-2486, 2010  
Preliminary version in IEEE Symp. on Foundations of Computer Science (FOCS), 2007  
**FOCS Special Issue**
9. Norms, XOR lemmas, and lower bounds for GF(2) polynomials and multiparty protocols  
With Avi Wigderson  
*Theory of Computing*, vol. 4, pp. 137-168, 2008  
Preliminary version in IEEE Conf. on Computational Complexity (CCC), 2007

8. On approximate majority and probabilistic time  
Computational Complexity, vol. 18, num. 3, pp. 337-375, 2009  
Preliminary version in IEEE Conf. on Computational Complexity (CCC), 2007
7. Pseudorandom Bits for Constant-Depth Circuits with Few Arbitrary Symmetric Gates  
SIAM J. on Computing, vol. 36, num. 5, pp. 1387-1403, 2007  
Preliminary version in 20th IEEE Conf. on Computational Complexity (CCC), 2005  
**SIAM Student Paper Prize**
6. On Constructing Parallel Pseudorandom Generators from One-Way Functions  
In 20th IEEE Conf. on Computational Complexity (CCC), 2005
5. Constant-Depth Circuits for Arithmetic in Finite Fields of Characteristic Two  
With Alexander Healy  
In 23rd Symp. on Theoretical Aspects of Computer Science (STACS), 2006
4. Fooling Parity Tests with Parity Gates  
With Dan Gutfreund  
In 8th Workshop on Randomization and Computation (RANDOM), 2004
3. Using Nondeterminism to Amplify Hardness  
With Alexander Healy and Salil P. Vadhan  
SIAM J. on Computing, vol. 35, num. 4, pp. 903-931, 2006  
Preliminary version in ACM Symp. on the Theory of Computing (STOC), 2004  
**STOC Special Issue**
2. The Complexity of Constructing Pseudorandom Generators from Hard Functions  
Computational Complexity, vol. 13, num. 3-4, pp. 147-188, 2004  
Preliminary version in IEEE Conf. on Computational Complexity (CCC), 2003
1. E-unifiability via Narrowing  
In 7th Italian Conference on Theoretical Computer Science (ICTCS), 2001

## **SURVEYS AND MY PH.D. THESIS**

All of the surveys below are peer reviewed.

4. Selected Results in Additive Combinatorics: An Exposition  
Theory of Computing Library, Graduate Surveys series, num. 3, pp. 1-15, 2011
3. On the power of small-depth computation  
Foundations and Trends in Theoretical Computer Science, vol. 5, num. 1, pp. 1-72, 2009  
Invited survey
2. Correlation bounds for polynomials over  $\{0, 1\}$   
SIGACT News, Complexity Theory Column, vol. 40, num. 1, 2009  
Invited survey
1. The Complexity of Hardness Amplification and Derandomization  
Ph.D. thesis, Harvard University, 2006

## NOTES

3. Think like the pros  
Manuscript, 2011  
Lecture notes aimed towards students lacking mathematical maturity
2. Reducing 3XOR to listing triangles, an exposition  
Manuscript, 2011
1. Gems of Theoretical Computer Science  
Manuscript, 2009  
Lecture notes of the class taught at Northeastern University

## OTHER WORKS BY RESEARCH GROUP

3. Information Spreading in Dynamic Networks  
Chinmoy Dutta and Gopal Pandurangan and Rajmohan Rajaraman and Zhifeng Sun  
Manuscript, 2011  
arXiv:1112.0384
2. Split and Join: Strong Partitions and Universal Steiner Trees for Graphs  
Costas Busch and Chinmoy Dutta and Jaikumar Radhakrishnan and Rajmohan Rajaraman and Srivathsan Srinivasagopalan  
Manuscript, 2011  
arXiv:1111.4766
1. More on a Problem of Zarankiewicz  
Chinmoy Dutta and Jaikumar Radhakrishnan  
Manuscript, 2011

## ACADEMIC VIDEO GAMES

### **ARORA: A Random Or Real Array**

2009

Web game to study the perception of randomness in financial data  
[www.ccs.neu.edu/home/viola/arora](http://www.ccs.neu.edu/home/viola/arora)

## TEACHING

**Northeastern University**, Boston, MA

*Theory of computation*

Spring 2010, Fall 2010, Spring 2011, Fall 2011

*Advanced algorithms*

Fall 2009, 2008

*Gems of theoretical computer science*

Spring 2009

## DEPARTMENTAL AND OTHER PROFESSIONAL SERVICE

<b>Faculty search committee</b> , joint Computer Science and Game Design position	2010 – 2011
<b>Faculty search committee</b> , joint Computer Science and Mathematics position	2009 – 2010
<b>Seminar organizer</b> , joint Boston University-Northeastern theory seminar	2008 – 2011
<b>Ph.D. committees</b> , Laura Poplawski (Northeastern), Joshua Brody (Dartmouth)	2008 – 2009
<b>Local co-organizer</b> , 25th IEEE Conference on Computational Complexity	CCC 2010
<b>Scientific board</b> , Electronic Colloquium on Computational Complexity	2009 – present

## COMMERCIAL VIDEO GAMES

<b>Black Viper</b> , distributed by Neo Software Produktions GmbH, Vienna, Austria	1994 – 1996
<b>Nathan Never</b> , distributed by Softel Ltd., Rome, Italy	1992

## INVITED TALKS

10. **Bertinoro workshop** on Ramsey Theory, Bertinoro, Italy  
The disproof of the inverse conjecture for Gowers' norm via Ramsey Theory Summer 2011
9. **Dagstuhl seminar** on the complexity of discrete problems, Wadern, Germany  
Extractors for circuit sources Spring 2011
8. **Banff workshop** on complexity theory, Banff, Canada  
The complexity of distributions Summer 2010
7. **Ohio State Univ. Conference**, in honor of Laci Babai's 60th birthday, Columbus, OH  
The complexity of distributions Spring 2010
6. **Banff workshop** on analytic tools in computational complexity, Banff, Canada  
Hardness amplification proofs require majority Summer 2008
5. **Cornell University workshop** on discrete harmonic analysis, Ithaca, NY  
Polynomials Spring 2008
4. **IBM Research/NYU/Columbia Theory Day**, New York, NY  
Polynomials Fall 2007
3. **Oberwolfach meeting** on complexity theory, Oberwolfach, Germany  
One-way multi-party communication lower bound for pointer jumping Summer 2007
2. **Dagstuhl seminar** on the complexity of boolean functions, Wadern, Germany  
On approximate majority and probabilistic time Spring 2007
1. **American Math. Society meeting** on randomness in computation, Lincoln, NE  
Pseudorandom bits for low complexity classes: new results and applications Fall 2005

## CONFERENCE AND SEMINAR TALKS

48. IEEE Symp. on Foundations of Computer Science, Palm Springs, CA  
Extractors for circuits sources FOCS; Fall 2011
47. IEEE Symp. on Foundations of Computer Science, Palm Springs, CA  
Randomness buys depth for approximate counting FOCS; Fall 2011
46. Northeastern University, Boston, MA  
The communication complexity of addition NEU; Fall 2011
45. Massachusetts Institute of Technology, Cambridge, MA  
The complexity of distributions MIT; Spring 2011
44. Northeastern University, Boston, MA  
Williams' breakthrough NEU; 16 November 2010
43. IEEE Symp. on Foundations of Computer Science, Las Vegas, NV  
The complexity of distributions FOCS; Fall 2010
42. La Sapienza University, Rome, Italy  
The complexity of distributions La Sapienza; Summer 2010
41. Microsoft Research New England  
The complexity of distributions Microsoft; Spring 2010
40. Harvard University, Cambridge, MA  
Lower bounds for succinct data structures Harvard; Fall 2009
39. La Sapienza University, Rome, Italy  
Lower bounds for succinct data structures La Sapienza; Summer 2009
38. ACM Symp. on Theory of Computing, Bethesda, MD  
Bit-probe lower bounds for succinct data structures STOC; Spring 2009
37. Northeastern University, Boston, MA  
Bit-probe lower bounds for succinct data structures NEU; Spring 2009
36. Institute for Advanced Study, Princeton, NJ  
Bounded independence fools halfspaces IAS; Spring 2009
35. Northeastern University, Boston, MA  
What is a proof? What is knowledge? What is randomness? NEU; Fall 2008
34. Boston University, Boston, MA  
Polynomials over  $\{0, 1\}$  BU; Fall 2008
33. IEEE Conf. on Computational Complexity, College Park, MD  
The sum of  $d$  small-bias generators fools polynomials of degree  $d$  CCC; Summer 2008
32. ACM Symp. on Theory of Computing, Victoria, Canada  
Hardness amplification proofs require majority STOC; Spring 2008

31. Columbia University, New York, NY  
Hardness amplification proofs require majority Columbia; Spring 2008
30. Northeastern University, Boston, MA  
Pseudorandomness NEU; Spring 2008
29. University of Illinois at Chicago, Chicago, IL  
Polynomials UIC; Spring 2008
28. The University of Chicago, Chicago, IL  
Lower bounds UChicago; Spring 2008
27. Institute for Advanced Study, Princeton, NJ  
Hardness amplification proofs require majority IAS; Spring 2008
26. IEEE Symp. on Foundations of Computer Science, Providence, RI  
One-way multi-party communication lower bound for pointer jumping with applications FOCS; Fall 2007
25. IEEE Symp. on Foundations of Computer Science, Providence, RI  
Pseudorandom bits for polynomials FOCS; Fall 2007
24. Columbia University, New York, NY  
Selected results in additive combinatorics Columbia; Fall 2007
23. IEEE Conf. on Computational Complexity, San Diego, CA  
Norms, XOR lemmas, and lower bounds for GF(2) polynomials and multiparty protocols CCC; Summer 2007
22. IEEE Conf. on Computational Complexity, San Diego, CA  
On approximate majority and probabilistic time CCC; Summer 2007
21. New York University, New York, NY  
Pseudorandomness: New results and applications NYU; Spring 2007
20. Institute for Advanced Study, Princeton, NJ  
One-way multi-party communication lower bound for pointer jumping with applications IAS; Spring 2007
19. IBM Watson Research Center, Hawthorne, NY  
Pseudorandomness: New results and applications IBM; Spring 2007
18. Institute for Advanced Study, Princeton, NJ  
On approximate majority and probabilistic time IAS; Spring 2007
17. Center for Discrete Math. and Theor. C. S., Rutgers, NJ  
Norms, XOR lemmas, and lower bounds for GF(2) polynomials and multiparty protocols DIMACS; Spring 2007
16. Institute for Advanced Study, Princeton, NJ  
Norms, XOR lemmas, and lower bounds for GF(2) polynomials and multiparty protocols IAS; Spring 2007
15. Toyota Technical Institute at Chicago, Chicago, IL  
Derandomization: New results and applications TTI; Spring 2006

14. La Sapienza University, Rome, Italy La Sapienza; Spring 2006  
Derandomization: New results and applications
13. Harvard University, Cambridge, MA Harvard; Spring 2006  
On approximate majority and probabilistic time
12. Center for Math. and Comp. Science, Amsterdam, the Netherlands CWI; Summer 2005  
Pseudorandom bits for constant-depth circuits with few arbitrary symmetric gates
11. IEEE Conf. on Computational Complexity, San Jose, CA CCC; Summer 2005  
On constructing parallel pseudorandom generators from one-way functions
10. IEEE Conf. on Computational Complexity, San Jose, CA CCC; Summer 2005  
Pseudorandom bits for constant-depth circuits with few arbitrary symmetric gates
9. Berkeley University, Berkeley, CA, Berkeley; Spring 2005  
Pseudorandom bits for constant-depth circuits with few arbitrary symmetric gates
8. Microsoft Research, Mountain View, CA Microsoft; Spring 2005  
Pseudorandom bits for constant-depth circuits with few arbitrary symmetric gates
7. Harvard University, Cambridge, MA Harvard; Spring 2004  
Pseudorandom bits for constant-depth circuits with few arbitrary symmetric gates
6. Institute for Advanced Study, Princeton, NJ IAS; Fall 2004  
Using nondeterminism to amplify hardness
5. ACM Symp. on Theory of Computing, Chicago, IL STOC; Summer 2004  
Using nondeterminism to amplify hardness
4. Radcliffe Inst. for Adv. Study, Cambridge, MA Radcliffe; Fall 2003  
Using nondeterminism to amplify hardness
3. IEEE Conf. on Computational Complexity, Aarhus, Denmark CCC; Summer 2003  
The complexity of constructing pseudorandom generators from hard functions
2. Harvard University, Cambridge, MA Harvard; Spring 2003  
The complexity of constructing pseudorandom generators from hard functions
1. Harvard University, Cambridge, MA Harvard; Fall 2001  
E-unifiability via narrowing