

EMANUELE VIOLA

September 9, 2009

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

RESEARCH INTERESTS

Computational complexity theory, pseudorandomness, cryptography, finance

CURRENT POSITION

Northeastern University, Boston, MA
Assistant professor

Fall 2008 – present

RESEARCH POSITIONS

Columbia University, New York, NY
Postdoctoral fellow; Sponsor: Rocco Servedio

Fall 2007 – Summer 2008

Institute for Advanced Study, Princeton, NJ
Postdoctoral fellow; Sponsor: Avi Wigderson

Fall 2006 – Summer 2007

EDUCATION

Harvard University, Cambridge, MA
Ph.D. Computer Science; Advisor: Salil Vadhan

Fall 2001 – Summer 2006

La Sapienza University, Rome, Italy
B.S. Computer Science, *summa cum laude*

Fall 1995 – Spring 2000

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

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; Israel Science Foundation, 2009

Journal refereeing

SIAM J. on Computing (SICOMP)	Computational Complexity (CC)
J. of Computer and System Sciences (JCSS)	Theoretical Computer Science (TCS)
Theory of Computing (ToC)	

PAPERS

- [17] Cell-probe lower bounds for succinct partial sums
With Mihai Pătraşcu
In ACM-SIAM Symposium on Discrete Algorithms SODA 2010
- [16] Bounded independence fools halfspaces
With Ilias Diakonikolas, Parikshit Gopalan, Ragesh Jaiswal, and Rocco Servedio.
In IEEE Symp. on Foundations of Computer Science FOCS 2009
- [15] Bit-probe lower bounds for succinct data structures
Invited and submitted to *SIAM J. on Computing*, **STOC special issue**
In ACM Symp. on Theory of Computing, STOC 2009
- [14] Improved separations between nondeterministic and randomized multiparty communication
With Matei David and Toniann Pitassi
To appear in *Transactions on Computation Theory*
In Int. Workshop on Randomization and Computation RANDOM 2008
- [13] The sum of d small-bias generators fools polynomials of degree d
Computational Complexity 18(2): 209-217, 2009, CCC special issue
In IEEE Conf. on Computational Complexity, **Best Paper Award** CCC 2008
- [12] Hardness amplification proofs require majority
With Ronen Shaltiel
In ACM Symp. on Theory of Computing STOC 2008
Submitted to *SIAM J. on Computing*
- [11] One-way multi-party communication lower bound for pointer jumping with applications
With Avi Wigderson
To appear in *Combinatorica*; invited to **FOCS special issue**
In IEEE Symp. on Foundations of Computer Science FOCS 2007
- [10] Pseudorandom bits for polynomials
With Andrej Bogdanov
To appear in *SIAM J. on Computing*, **FOCS special issue**
In IEEE Symp. on Foundations of Computer Science FOCS 2007
- [9] Norms, XOR lemmas, and lower bounds for GF(2) polynomials and multiparty protocols
With Avi Wigderson
Theory of Computing 4:137-168, 2008.
In IEEE Conf. on Computational Complexity CCC 2007
- [8] On approximate majority and probabilistic time
To appear in *J. of Computational Complexity*
In IEEE Conf. on Computational Complexity CCC 2007
- [7] Pseudorandom bits for constant-depth circuits with few arbitrary symmetric gates
SIAM J. on Computing, 36(5):1387-1403, 2007, **SIAM Student Paper Prize 2006**
In IEEE Conf. on Computational Complexity CCC 2005
- [6] On constructing parallel pseudorandom generators from one-way functions
In IEEE Conf. on Computational Complexity CCC 2005

- [5] Constant-depth circuits for arithmetic in finite fields of characteristic two
 With Alexander Healy
 In Int. Symp. on Theoretical Aspects of Computer Science STACS 2006
- [4] Fooling parity tests with parity gates
 With Dan Gutfreund
 In Int. Workshop on Randomization and Computation RANDOM 2004
- [3] Using nondeterminism to amplify hardness
 With Alexander Healy and Salil Vadhan
SIAM J. on Computing, 35(4):903-931, 2006, **STOC special issue**
 In ACM Symp. on Theory of Computing STOC 2004
- [2] The complexity of constructing pseudorandom generators from hard functions
J. of Computational Complexity, 13(3-4):147-188, 2004
 In IEEE Conf. on Computational Complexity CCC 2003
- [1] E-unifiability via narrowing
 In Italian Conf. on Theoretical Computer Science ICTCS 2001

INVITED SURVEYS

- [2] On the power of small-depth computation
 Submitted to *Foundations and Trends in Theoretical Computer Science* 2009
- [1] Correlation bounds for polynomials over $\{0, 1\}$
 ACM SIGACT news 40(1) SIGACT 2009

TECHNICAL REPORTS

- [3] A computational view of market efficiency
 With Jasmina Hasanhodzic and Andrew W. Lo
 arXiv:0908.4580v1 arXiv 2009
- [2] Selected results in additive combinatorics: An exposition
 Submitted to *Theory of Computing*, graduate surveys
 Electronic Colloquium on Computational Complexity, Report 07-103 ECCC 2007
- [1] New correlation bounds for GF(2) polynomials using Gowers uniformity
 Electronic Colloquium on Computational Complexity, Report 06-097 ECCC 2006

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

TEACHING

- Northeastern University**, Boston, MA
Theory of computation Spring 2010
Advanced algorithms Fall 2009, 2008
Gems of theoretical computer science Spring 2009

DEPARTMENTAL AND OTHER PROFESSIONAL SERVICE

Seminar organizer, joint Boston University-Northeastern theory seminar 2008 – 2009
Ph.D. committees, Laura Poplawski (Northeastern), Joshua Brody (Dartmouth) 2008 – 2009
Local co-organizer, 25th IEEE Conference on Computational Complexity CCC 2010

COMMERCIAL VIDEO GAMES

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

INVITED TALKS

[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

[39] La Sapienza University, Rome, Italy La Sapienza; Summer 2009
Lower bounds for succinct data structures

[38] ACM Symp. on Theory of Computing, Victoria, Canada STOC; Spring 2009
Bit-probe lower bounds for succinct data structures

[37] Northeastern University, Boston, MA NEU; Spring 2009
Bit-probe lower bounds for succinct data structures

[36] Institute for Advanced Study, Princeton, NJ IAS; Spring 2009
Bounded independence fools halfspaces

[35] Northeastern University, Boston, MA NEU; Fall 2008
What is a proof? What is knowledge? What is randomness?

[34] Boston University, Boston, MA BU; Fall 2008
Polynomials over $\{0, 1\}$

[33] IEEE Conf. on Computational Complexity, College Park, MD CCC; Summer 2008
The sum of d small-bias generators fools polynomials of degree d

[32] ACM Symp. on Theory of Computing, Victoria, Canada STOC; Spring 2008
Hardness amplification proofs require majority

[31] Columbia University, New York, NY Columbia; Spring 2008
Hardness amplification proofs require majority

- [30] Northeastern University, Boston, MA NEU; Spring 2008
Pseudorandomness
- [29] University of Illinois at Chicago, Chicago, IL UIC; Spring 2008
Polynomials
- [28] The University of Chicago, Chicago, IL UChicago; Spring 2008
Lower bounds
- [27] Institute for Advanced Study, Princeton, NJ IAS; Spring 2008
Hardness amplification proofs require majority
- [26] IEEE Symp. on Foundations of Computer Science, Providence, RI FOCS; Fall 2007
One-way multi-party communication lower bound for pointer jumping with applications
- [25] IEEE Symp. on Foundations of Computer Science, Providence, RI FOCS; Fall 2007
Pseudorandom bits for polynomials
- [24] Columbia University, New York, NY Columbia; Fall 2007
Selected results in additive combinatorics
- [23] IEEE Conf. on Computational Complexity, San Diego, CA CCC; Summer 2007
Norms, XOR lemmas, and lower bounds for $GF(2)$ polynomials and multiparty protocols
- [22] IEEE Conf. on Computational Complexity, San Diego, CA CCC; Summer 2007
On approximate majority and probabilistic time
- [21] New York University, New York, NY NYU; Spring 2007
Pseudorandomness: New results and applications
- [20] Institute for Advanced Study, Princeton, NJ IAS; Spring 2007
One-way multi-party communication lower bound for pointer jumping with applications
- [19] IBM Watson Research Center, Hawthorne, NY IBM; Spring 2007
Pseudorandomness: New results and applications
- [18] Institute for Advanced Study, Princeton, NJ IAS; Spring 2007
On approximate majority and probabilistic time
- [17] Center for Discrete Math. and Theor. C. S., Rutgers, NJ DIMACS; Spring 2007
Norms, XOR lemmas, and lower bounds for $GF(2)$ polynomials and multiparty protocols
- [16] Institute for Advanced Study, Princeton, NJ IAS; Spring 2007
Norms, XOR lemmas, and lower bounds for $GF(2)$ polynomials and multiparty protocols
- [15] Toyota Technical Institute at Chicago, Chicago, IL TTI; Spring 2006
Derandomization: New results and applications
- [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
Pseudorandom bits for constant-depth circuits with few arbitrary symmetric gates
- [10] Berkeley University, Berkeley, CA Berkeley; Spring 2005
Pseudorandom bits for constant-depth circuits with few arbitrary symmetric gates

- [9] Microsoft Research, Mountain View, CA Microsoft; Spring 2005
Pseudorandom bits for constant-depth circuits with few arbitrary symmetric gates
- [8] Harvard University, Cambridge, MA Harvard; Spring 2004
Pseudorandom bits for constant-depth circuits with few arbitrary symmetric gates
- [7] IEEE Conf. on Computational Complexity, San Jose, CA CCC; Summer 2005
On constructing parallel pseudorandom generators from one-way functions
- [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