

Joshua Brody

CONTACT INFORMATION	Swarthmore College Computer Science Department 500 College Ave Swarthmore, PA 19081	609 Elm Ave. Swarthmore, PA 19081 www.cs.swarthmore.edu/~brody joshua.e.brody@gmail.com (610)-690-6866
RESEARCH INTERESTS	Theoretical Computer Science, including communication complexity, unconditional lower bounds, query complexity, property testing, streaming algorithms, data structures.	
EDUCATION	Dartmouth College , Hanover, NH Ph.D., “Some Communication Complexity Results and Their Applications” Advisor: Amit Chakrabarti Research Area: Communication Complexity <i>2005-2010</i>	
	New York University , New York, NY Master of Science in Computer Science GPA: 3.97/4.0 <i>2003-2005</i>	
	Carnegie Mellon University , Pittsburgh, PA Bachelor of Science in Mathematics/Computer Science GPA: 3.32/4.0 <i>1993-1997</i>	
EMPLOYMENT	Swarthmore College , Swarthmore, PA Associate Professor Assistant Professor Visiting Assistant Professor Rutgers University DIMACS , New Brunswick, NJ Visiting Scholar University of Waterloo , Waterloo, Canada Visiting Assistant Professor Aarhus University , Aarhus, Denmark Postdoctoral researcher, Computer Science Supervisor: Peter Bro Miltersen Tsinghua University IIS , Beijing, China Postdoctoral researcher at the Institute for Interdisciplinary Information Sciences Supervisor: Andrew Chi-Chih Yao Dartmouth College , Hanover, NH Lecturer for Computer Architecture (CS 37) Research Assistant Encoda Systems , New York, NY Software Developer Lycée Provincial de Yako , Yako, Burkina Faso Peace Corps Volunteer (Secondary Math Education) Lockheed Martin ATL , Camden, NJ Software Engineer	<i>2020-present</i> <i>2014-2020</i> <i>2013-2014</i> <i>2022</i> <i>2017-2018</i> <i>2011-2013</i> <i>2010-2011</i> <i>2010</i> <i>2006-2010</i> <i>2003-2004</i> <i>2000-2002</i> <i>1998-2000</i>

GRANTS
AND FUNDING

Eugene M. Lang Faculty Fellowship. For second semester sabbatical support. 2018.
Lower Bounds via Communication Complexity. Danish Council for Independent Research. DKK 1,718,502 (\$318,000). October 2011-June 2013.

JOURNAL
PUBLICATIONS

Undergraduate coauthors indicated with a (*).

[J5] "A Strong XOR Lemma for Randomized Query Complexity", (with **Jae Tak Kim***, **Peem Lerdputtipongporn***, and **Hariharan Srinivasulu***), *Theory of Computing*, 2023.

[J4] "Certifying Equality With Limited Interaction", (with Amit Chakrabarti, Ranganath Kondapally, David P. Woodruff, and Grigory Yaroslavtsev), *Algorithmica*, **76**(19), 2016, pp. 796-845. Special issue on Information Complexity and Applications. (see [C16] and [C18] below)

[J3] "Towards a Reverse Newman's Theorem in Interactive Information Complexity", (with Harry Buhrman, Michal Koucky, Bruno Loff, Florian Speelman, and Nikolay Vereshchagin), *Algorithmica*, **76**(19), 2016, pp. 749-781. Special Issue on Information Complexity and Applications. (see [C14] below)

[J2] "Adapt or Die: Polynomial Lower Bounds for Nonadaptive Data Structures," (with Kasper Green Larsen), *Theory of Computing*, **11**(19), 2015, pp. 471-489.

[J1] "Property Testing Lower Bounds via Communication Complexity," (with Eric Blais and Kevin Matulef), *Computational Complexity*, **21**(2), 2012, pp. 311-358. Special issue of selected papers from the 26th IEEE Conference on Computational Complexity (CCC 2011). (see [C9] below)

CONFERENCE
PUBLICATIONS

Undergraduate coauthors indicated with a (*).

[C22] "Optimal Separation and Strong Direct Sum for Randomized Query Complexity." (with Eric Blais), in *34th IEEE Conference on Computational Complexity (CCC 2019)*.

[C21] "Non-Adaptive Data Structures for Predecessor Search." (with **Joe Boninger*** and **Owen Kephart***), in *37th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2017)*.

[C20] "Position-Based Cryptography and Multiparty Communication." (with Stefan Dziembowski, Sebastian Faust, and Krzysztof Pietrzak), in *15th IACR Theory of Cryptography Conference (TCC 2017)*.

[C19] "Dependent Random Graphs and Multi-Party Pointer Jumping," (with **Mario Sanchez***), in *19th International Workshop on Randomization and Computation (RANDOM 2015)*.

[C18] "Certifying Equality with Limited Interaction," (with Amit Chakrabarti, Ranganath Kondapally, David P. Woodruff, and Grigory Yaroslavtsev), in *18th International Workshop on Randomization and Computation (RANDOM 2014)*. **Invited to the Special Issue of Algorithmica on Information Complexity and Applications**. (see [J4] above)

[C17] "The Information Complexity of Hamming Distance," (with Eric Blais and Badih Ghazi), in *18th International Workshop on Randomization and Computation (RANDOM 2014)*.

[C16] "Beyond Set Disjointness: The Communication Complexity of Finding the Intersection," (with Amit Chakrabarti, Ranganath Kondapally, David P. Woodruff, and Grigory Yaroslavtsev), in *33rd Annual ACM Symposium on Principles of Distributed Computing (PODC 2014)*. **Invited to the Special Issue of Algorithmica on Information Complexity and Applications**. (see [J4] above)

[C15] “Cryptogenography,” (with Sune Jakobsen, Dominik Scheder, and Peter Winkler), in *5th Innovations in Theoretical Computer Science (ITCS 2014)*.

[C14] “Towards a Reverse Newman’s Theorem in Interactive Information Complexity,” (with Harry Buhrman, Michal Koucky, Bruno Loff, Florian Speelman, and Nikolay Vereshchagin), in *28th IEEE Conference on Computational Complexity (CCC 2013)*. **Invited to the Special Issue of Algorithmica on Information Complexity and Applications.** (see [J3] above)

[C13] “Space-Bounded Communication Complexity,” (with Shiteng Cheng, Periklis A. Papakonstantinou, Hao Song, and Xiaoming Sun), in *4th Innovations in Theoretical Computer Science (ITCS 2013)*.

[C12] “Space Efficient Approximation Scheme for Circular Earth Mover Distance,” (with Hongyu Liang and Xiaoming Sun), in *10th Latin American Theoretical Informatics Symposium (LATIN 2012)*.

[C11] “Streaming Algorithms with One-Sided Estimation,” (with David P. Woodruff), in *15th International Workshop on Randomization and Computation (RANDOM 2011)*.

[C10] “Lower Bounds for Testing Computability by Small Width OBDDs,” (with Kevin Matulef and Chenggang Wu), in *8th Annual Conference on Theory and Applications of Models of Computation (TAMC 2011)*.

[C9] “Property Testing Lower Bounds via Communication Complexity,” (with Eric Blais and Kevin Matulef), in *26th Annual IEEE Conference on Computational Complexity (CCC 2011)*. **Invited to the Special Issue of Computational Complexity.** (see [J1] above)

[C8] “The Coin Problem and Pseudorandomness for Branching Programs,” (with Elad Verbin), in *51st Annual IEEE Symposium on Foundations of Computer Science (FOCS 2010)*.

[C7] “Better Gap Hamming Lower Bounds via Better Round Elimination,” (with Amit Chakrabarti, Oded Regev, Thomas Vidick, and Ronald de Wolf), in *14th International Workshop on Randomization and Computation (RANDOM 2010)*.

[C6] “Distributed Monitoring of Conditional Entropy for Anomaly Detection in Streams,” (with Chrisil Arackaparambil, Sergey Bratus, and Anna Shubina), in *3rd International Workshop on Scalable Stream Processing Systems (SSPS 2010)*.

[C5] “A Multi-Round Communication Lower Bound for Gap Hamming and Some Consequences,” (with Amit Chakrabarti), in *24th Annual IEEE Conference on Computational Complexity (CCC 2009)*.

[C4] “The Maximum Communication Complexity of Multiparty Pointer Jumping,” (sole author), in *24th Annual IEEE Conference on Computational Complexity (CCC 2009)*.

[C3] “Functional Monitoring Without Monotonicity,” (with Chrisil Arackaparambil and Amit Chakrabarti), in *36th International Colloquium on Automata, Languages, and Programming (ICALP 2009)*.

[C2] “Streaming Estimation of Information-theoretic Metrics for Anomaly Detection,” (with Sergey Bratus, David Kotz, and Anna Shubina), in *11th International Symposium on Recent Advances in Intrusion Detection (RAID 2008)*.

[C1] “Sublinear Communication Protocols for Multi-Party Pointer Jumping and a Related Lower Bound,” (with Amit Chakrabarti), in *25th International Symposium on Theoretical Aspects of Computer Science (STACS 2008)*.

MANUSCRIPTS

[M2] “Dependent Random Graph Properties via Jumbledness.” (with Aditi Dudeja), 2023.

[M1] “Graph Containment Properties in Dependent Random Graphs.” (with **Mario Sanchez***), 2016.

TEACHING
EXPERIENCE

Swarthmore College, Swarthmore, PA
CPSC 21: Introduction to Computer Science F21, S19, S16
CPSC 35: Data Structures and Algorithms S24, F23, S20, S17, F14, S14
CPSC 35: Data Structures and Algorithms (lab obly) Fall 2013
CPSC 41: Algorithms F22, F20, F19, F18, F16, S15, F13
CPSC 49/MATH 59: The Probabilistic Method Fall 2015
CPSC 91T: Randomized Algorithms Spring 2023
CPSC 93: Directed Reading: Competitive Programming F23, S23, F22
CPSC 93: Directed Reading: Cryptogenography Spring 2019, Spring 2016
CPSC 93: Directed Reading: Randomness and Computation Spring 2019, Fall 2018
CPSC 93: Directed Reading: Random Graph Theory Fall 2015, Fall 2014
CPSC 93: Directed Reading: Communication Complexity II Spring 2014
CPSC 93: Directed Reading: Communication Complexity I Fall 2013

Aarhus University, Aarhus, Denmark
Sublinear Time Algorithms: Property Testing Winter 2013
Communication Complexity Fall 2011

KTH Royal Institute of Technology, Stockholm, Sweden
Seminars on Theoretical Computer Science: Communication Complexity September 2012
Guest Lecturer, six hours total. Primary Instructor: Jakob Nordström.

Tsinghua University IIS, Beijing, China
Yao Class Research Immersion Course in Theoretical Computer Science Summer 2011

Dartmouth College, Hanover NH
CS37: Computer Architecture Summer 2010
CS4: Concepts in Computing (Teaching Assistant) Spring 2006
CS5: Introduction to Computer Science (Teaching Assistant) Fall 2005, Fall 2006
CS37: Computer Architecture (Teaching Assistant) Spring 2010

Lycée Provincial de Yako, Yako, Burkina Faso
Junior/Senior High School Mathematics (instruction in French) 2000-2002

HONORS
THESES

Joseph Boninger (Highest Honors, 2016).
“New Bounds for the Memoryless and Nonadaptive Dynamic Predecessor Problems”.

SUMMER
RESEARCH
STUDENTS

Zachary Potthoff, Zheyao Yao (2024). “Randomized Query Complexity of Recursive Majority”.

Runze Wang (2020). “Strong Direct Sum for Majority”.

Jae Tak Kim, Peem Lerdupttipongporn, Hari Srinivasulu (2019). “Randomized Query Complexity”.

Alex Crane (2016). “Cryptogenography”.

Joseph Boninger, Owen Kephart (2015). “Non-adaptive Data Structures”.

Mario Sanchez (2014). “Dependent Random Graphs and Multiparty Pointer Jumping”.

KJ Bredder (2014). “Cryptogenography”.

UNIVERSITY
ACTIVITIES

Swarthmore College

Financial Compensation Committee (2024)
Writing Associates Programm Advising Committee (2023-2024)
Provost Search Committee (2022-2023)
Endowed Funds Committee (2022-2023)
NSE Inclusive Excellence Committee (2019-2020)
Swat FLI Navigator (2019-2020)
Coach of the ICPC Programming Team (2014-2016, 2018-present)

- 46-th World Finals Luxor 2023 (declined).
- 45-th World Finals Dhaka 2022 (T26th place).
- World Finals Invitational 2021 (4th place).
- North American Championships 2022 (2nd), 2021 (4th), 2020 (9th).

Fellowships and Prizes Committee (2018-2019)
Grace Hopper Celebration Department Coordinator (2016)
Sigma Xi Treasurer, Swarthmore College Chapter (2015-2017)
Aydelotte Foundation Faculty Seminar in Pedagogy (2016-2017)
Aydelotte Foundation Faculty Seminar in Collaboration (2015-2016)
ITS Committee (2014-2015)

Tsinghua University IIS

Organizer, Theory Lunch (2010-2011)
Organizer, Algorithms, Complexity, Cryptography Seminar (2011)

Dartmouth College

Ph.D. Admissions Committee, student member (2006, 2008)
Co-founder and organizer, Dartmouth Computer Science Research Symposium (2006,2007)

PROFESSIONAL
SERVICE

Review Panel Member: National Science Foundation (2020, 2019)
Program Committee Member: RANDOM 2018
Workshop Co-Organizer: CTIC Workshop on Synergies in Lower Bounds (2009)
Funding Reviewer: Czech Science Foundation, Israeli Science Foundation.
Journal Referee: Algorithmica, Computational Complexity, DIST, JACM, Journal of Cryptography, SICOMP, Theory of Computing, Theory of Computing Systems, Transactions on Computation Theory, Transactions on Information Theory.
Conference Referee: APPROX, CCC, DISC, FOCS, ICALP, ITCS, PODS, RANDOM, SIROCCO, SODA, SOFSEM, SPAA, STACS, STOC.

INVITED
WORKSHOPS

Simons Institute Workshop on Interactive Complexity, University of California, Berkeley, CA. October 2018.
BIRS Workshop on Communication Complexity and Applications, Banff International Research Station, Banff, Canada. March 2017.
IMS Workshop on Log Rank Conjecture, IMS, Singapore. January 2016.
BIRS Workshop on Communication Complexity and Applications, Banff International Research Station, Banff, Canada. August 2014. **Tutorial Speaker.**

INVITED
TALKS

“Strong Direct Sum for Randomized Query Complexity,” *DIMACS Theoretical Computer Science Seminar*, Rutgers University, New Brunswick, NJ. April 2019.

“Strong Direct Sum for Randomized Query Complexity,” *Simons Institute Workshop on Interactive Complexity*, University of California, Berkeley, CA. October 2018.

“Dependent Random Graphs and Multiparty Pointer Jumping,” *University of Waterloo Algorithms and Complexity Seminar*, Waterloo, Canada. February 2018.

“Non-Adaptive Data Structure Bounds for Dynamic Predecessor,” *BIRS Workshop on Communication Complexity and Applications*, Banff, Canada. March 2017.

“Dependent Random Graphs and Multiparty Pointer Jumping,” *Johns Hopkins Algorithms and Complexity Seminar*, Baltimore, MD. March 2016.

“Dependent Random Graphs and Multiparty Pointer Jumping,” *IMS Workshop on Log Rank Conjecture*, Institute For Mathematical Sciences, Singapore. January 2016.

“Dependent Random Graphs and Multiparty Pointer Jumping,” *University of Pennsylvania Theory Seminar*, Philadelphia, PA. December 2015.

“Property Testing Lower Bounds via Communication Complexity,” *BIRS Workshop on Communication Complexity and Applications*, Banff, Canada. August 2014.

“Certifying Equality with Limited Interaction” *Aarhus University Theory Seminar*, Aarhus, Denmark. October 2012.

“Communication Complexity and Lower Bounds in Computer Science,” *Aarhus University Friday Lecture*, Aarhus, Denmark. October 2012.

“Amazingly Dense Ruzsa-Szemerédi Graphs, Plus Applications,” *KTH Theory Reading Group*, Stockholm, Sweden. September 2012.

“Streaming Algorithms with One-Sided Estimation,” *TU Dortmund Workshop on Algorithms for Data Streams*, Dortmund, Germany. July 2012.

“Property Testing Lower Bounds via Communication Complexity: A Survey,” *Centrum Wiskunde & Informatica (CWI)*, Amsterdam, Netherlands. March 2012.

“Property Testing Lower Bounds via Communication Complexity: A Survey,” *LIAFA Theory Seminar*, Paris, France. March 2012.

“Property Testing Lower Bounds via Communication Complexity,” *University of Massachusetts-Amherst Theory Seminar*, Amherst, MA. June 2011.

“Property Testing Lower Bounds via Communication Complexity,” *Dartmouth College Theory Seminar*, Hanover, NH. June 2011.

“Communication Complexity and Applications,” *Tsinghua University ITCS Institute Seminar*, Beijing, China. September 2010.

“Better Gap Hamming Lower Bounds via Better Round Elimination,” *University of Massachusetts-Amherst Theory Seminar*, Amherst, Massachusetts. February 2010.

“The NOF Communication Complexity of Multi-Party Pointer Jumping,” *Institute for Advanced Study (IAS) Computer Science/Discrete Mathematics Seminar*, Princeton, NJ. December 2009.

“Multiround Lower Bounds for Gap Hamming via Round Elimination,” *Aarhus University*, Aarhus, Denmark. November 2009.

“The NOF Communication Complexity of Multi-Party Pointer Jumping,” *Aarhus University*, Aarhus, Denmark. November 2009.

“Lower Bounds for Gap-Hamming-Distance and Consequences for Streaming Algorithms,” *Centrum Wiskunde & Informatica (CWI)*, Amsterdam, Netherlands. July 2009.

“A Multi-Round Communication Lower Bound for the Gap Hamming Problem,” *Tel Aviv University Theory of Computation Seminar*, Tel Aviv, Israel. June 2009.

“Some Applications of Communication Complexity,” *Northeastern University Theory of Computation Seminar*, Boston, MA. February 2009.