Johan Håstad

July 2011

1 Address

Skolan för datavetenskap och kommunikation
Kungliga Tekniska Högskolan
100 44 Stockholm, SWEDEN
46-8-790 6289, fax: 46-8-790 0930
email:johanh@kth.se

2 Research Interests

Theory of computation. In particular, complexity theory, lower bounds, cryptography and pseudorandomness, randomized algorithms and approximation algorithms.

3 Personal Data

Born 1960. Married, 2 children. Swedish citizen.

4 Education

- Bachelor of Science (Högskoleexamen) with major in mathematics, Stockholm University, 1981.
- Master of Science (Licentiat) in Mathematics, Uppsala University, 1984.
- Ph. D. in Mathematics, MIT, 1986.
- Accepted as "oavlönad docent" in Computer Science at the Royal Institute of Technology, 1988.

5 Major Awards and honors

- ACM Doctoral Dissertation Award, 1986.
- Swedish Mathematical Society's stipend, 1986.
- Chester Carlson's research prize, 1990.
- Gödel prize, 1994.
- Invited speaker at the ICM, Berlin, 1998.
- Göran Gustafsson prize in mathematics, 1999.
- Plenary speaker at the ECM, Stockholm, 2004.
- Gödel prize, 2011.

6 Commissions of trust

- Member of the Royal Swedish Academy of Sciences, 2001.
- Member of the board of the school of Computer Science and Communication at KTH, 2005-2011.
- Vice director of SSF-center Center for Industrial and Applied Mathematics, CIAM, 2006-.
- Member of the Nevanlinna Prize Committee, ICM, 2006.
- Member of "NT-rådet" at "Vetenskapsrådet", 2007-2009. (a position at the Research Council, the major funder of basic research in Sweden).
- Member of Gödel Prize committee, representative of SIGACT 2008-2010.
- Chairman of the board, Stockholm Mathmatics Center, 2009-

7 Research funding

Has continuously held a grant from Swedish grant agencies TFR and VR, starting in the 1990'ies. Has recently obtained an advanced investigator grant from ERC, for the period 2009-2013 and the total amount 2370 KEUR.

8 Visiting position

- Visiting scientist, fall 1994, Massachusetts Institute of Technology.
- Member for academic year 2000/2001, Institute for Advanced Study, Princeton.

9 Employment after Ph.D

- Post Doc position, (1986-1987), Massachusetts Institute of Technology.
- Associate Professor[1], (1988-1992), Kungl Tekniska Högskolan.
- Full Professor[2], (1992-), Kungl Tekniska Högskolan.

10 Editorial positions

Currently an editor of:

- *Computational Complexity* (since 1991).
- *Theory of Computing*, open access journal (since 2004).
- *Random Structures and Algorithms*, (since 2008).
- *ACM Transactins on Computation Theory*, (since 2008).

Previously an editor for *Information Processing Letter* (1990-1993), *SIAM Journal on Computing* (1991-1999), and *Journal of the ACM* (1997-2003).
Member of the scientific board of *Electronic Colloquium on Computational Complexity*.

11 Program Committees

Served as a member of the following program committees:

Eurocrypt 1989, SWAT 1990, STACS 1991, STOC 1992, ICALP 1993, NFRs beredningsgrupp i matematik 1993-95 (Swedish grant agency), FOCS 1994, ESA 1996, TFRs beredningsgrupp i datalogi 1996 (Swedish grant agency), CRYPTO 1998, Approx 1998, ICALP 2002, CRYPTO 2002, STOC 2003, Computational Complexity 2003, FOCS 2004, Eurocrypt 2005, Random 2005, Theory of Cryptography Conference 2006, ICALP 2006, Approx 2006, SWAT 2008, ESA 2008, Computational Complexity 2009 (chair), Theory of Cryptography Conference 2010, Crypto 2010.

12 Advising

Honors for supervised graduate students

- Jonas Holmerin, "Best Ph.D-thesis in Sweden in Computer Science during 2002" prize by Naturvetarförbundet.
- Jakob Nordström, shared "Best student paper"-award at STOC 2006.

[1] Högskolelektor med forskningsinriktning
[2] Professor i teoretisk datalogi

- Per Austrin, "Best student paper"-award (Machtey-prize) at FOCS 2007.
- Jakob Nordström, Ackermann award 2009, given out by EACSL for for outstanding thesis Ph.D thesis in Logic in Computer Science.

Currently supervising 5 students, completed Ph. D.-theses supervised:

- Viggo Kann "On the Approximability of NP-complete Optimization Problems" May 1992.
- Mikael Goldmann "On Threshold Circuits and Related Models of Computation" December 1992.
- Christer Berg "On Oracles and Circuits – Topics in Computational Complexity" December 1997.
- Mats Näslund "Bit Extraction, Hard-Core Predicates, and the Bit Security of RSA", October 1998.
- Staffan Ulfberg "On Lower Bounds for Circuits and Selection", December 1999.
- Jonas Holmerin "On Probabilistic Proof Systems and Hardness of Approximation", December 2002.
- Gustav Hast "Beating a Random Assignment", June 2005.
- Douglas Wikström "On the security of Mix-Nets and Hierarchical Group Signatures", December 2005.
- Mårten Trolin "Electronic Cash and Hierarchical Group Signatures", December 2006.
- Jakob Nordström "Short proofs may be spacious: Understanding space in resolution", May 2008.
- Per Austrin "Conditional Inapproximability and Limited Independence", November 2008.
- Gunnar Kreitz "Aspects of Secure and Efficient Streaming and Collaboration", May 2011.

Completed Licentiate-theses supervised, who have not completed a Ph.D under my supervision.

- Lars Arvestad "Adapting to nature – some improvements on alignment algorithms in computational biology", October 1997.
- Anna Redz "On equality testing protocols and their security", September 2003.
- Rafael Pass "Alternativ variants of zero-knowledge proofs", January 2005.

13 Patents

- Patent nr 512.279 "Elektroniska transaktionssystem", Swedish patent, granted Februari 2000. Co-inventor Stefan Hellberg.

14 Journal Publications

[J1] J. Lagarias and J. Håstad "Simultaneous Diophantine Approximations of Rationals by Rationals", *Journal of Number Theory*, 1985, Vol 24, No 2, pp 200–228.

[J2] R. Boppana, J. Håstad and S. Zachos "Does co-NP have Short Interactive Proofs'?', *Information Processing Letters*, Vol. 25, No 2, May 1987, pp 127–132.

[J3] J. Håstad "Oneway Permutations in NC^0", *Information Processing Letters*, 1987/88, Vol 26, pp 153–155.

[J4] A. Frieze, J. Håstad, R. Kannan, J. Lagarias and A. Shamir "Reconstructing Truncated Integer Variables Satisfying Linear Congruences", *SIAM Journal on Computing*, 1988, Vol. 17, No 2, pp 262–280.

[J5] J. Håstad "Solving Simultaneous Modular Equations of Low Degree", *SIAM Journal on Computing*, 1988, Vol. 17, No 2, pp 336–341.

[J6] J. Håstad "Dual Vectors and Lower Bounds for the Nearest Lattice Point Problem", *Combinatorica*, Vol 8, No 1, 1988, pp 75–81.

[J7] J. Håstad "Lower Bounds in Computational Complexity Theory", *Notices of the AMS*, Vol. 35, No 5, 1988, pp 677–683.

[J8] J. Håstad, B. Just, J. Lagarias, and C. Schnorr "Polynomial Time Algorithms for Finding Integer Relations Among Real Numbers", *SIAM Journal on Computing*, 1989, Vol 18, No 5, pp 859–881.

[J9] J. Håstad "Almost Optimal Lower Bounds for Small Depth Circuits", in *Randomness and Computation*, Advances in Computing Research, Vol 5, ed. S. Micali, 1989, JAI Press Inc, pp 143–170.

[J10] P. Beame and J. Håstad "Optimal Bounds for Decision Problems on the CRCW PRAM", *Journal of ACM*, 1989, Vol 36, No 3, pp 643–670.

[J11] J. Håstad "Tensorrank is NP-complete", *Journal of Algorithms*, 1990, Vol 11, pp 644–654.

[J12] W. Aiello, J. Håstad and S. Goldwasser "On the Power of Interaction", *Combinatorica*, 1990, Vol 10, No 1, pp 3–25.

[J13] J. Håstad and J. Lagarias "Simultaneously Good Bases of a Lattice and its Reciprocal Lattice", *Mathematische Annalen* 287, 1990, pp 163–174.

[J14] J. Håstad and M. Goldmann "On the Power of Small-Depth Threshold Circuits", *Computational Complexity*, Vol 1, 1991, pp 113–129.

[J15] W. Aiello and J. Håstad "Statistical Zero-Knowledge Languages can be Recognized in Two Rounds", *Journal of Computer and System Sciences*, Vol 42, 1991, pp 327–345.

[J16] W. Aiello and J. Håstad "Relativized Perfect Zero-Knowledge is not BPP", *Information and Computation*, 1991, Vol 93, No 2, pp 223–240.

[J17] M. Goldmann, J. Håstad and A. Razborov "Majority Gates vs. General Weighted Threshold Gates", *Journal of Computation Complexity*, 1992, Vol 1, No 4, pp 277–300.

[J18] N. Alon, O. Goldreich, J. Håstad and R. Peralta. "Simple Constructions of Almost k-wise Independent Random Variables", *Random Stuctures and Algorithms*, Vol 3, No 3, 1992, pp 289–304.

[J19] M. Goldmann and J. Håstad, "A Simple Lower Bound for the Depth of Monotone Circuits Computing Clique using a Communication Game", *Information Processing Letters*, Vol 41, No 4, 1992, pp 221–226.

[J20] J. Håstad, A. Schrift och A. Shamir. "The Discrete Logarithm Modulo a Composite Hides $O(n)$ bits", *Journal of Computer and System Science*, 1993, Vol 47, No 3, pp 376–404.

[J21] J. Håstad and A. Wigderson, "Composition of the Universal Relation", in "Advances in Computational Complexity Theory", AMS-DIMACS book series, Volume 13, 1993 ed. J-Y. Cai, pp 119–134.

[J22] J. Håstad, S. Phillips and S. Safra, "A Well Characterized Approximation Problem", *Information processing letters*, Vol 47:6, 1993 pp. 301–305.

[J23] M. Goldmann, P. Grape, and J. Håstad, "On Average Time Hierarchies", *Information processing letters*, Vol 49:1, 1994, pp 15–20.

[J24] R. Chang, B. Chor, O. Goldreich, J. Hartmanis, J. Håstad, D. Ranjan and P. Rohatgi. "The Random Oracle Hypothesis is False", *Journal of Computer and System Sciences*, Volume 49, No 1, 1994 pp 24–39.

[J25] J. Håstad, J. Lagarias, and A. Odlyzko, "On the Distribution of Multiplicative Translates of Sets of Residues (mod p)", *Journal on Number Theory*, Vol 46, No 1, 1994, pp 108–122.

[J26] J. Håstad, I. Wegener, N. Wurm and S. Yi, "Optimal Depth, very Small Size Circuit for Symmetric Functions in AC^0, *Information and Computation*, Volume 108, No 2, 1994, pp 200–211.

[J27] J. Håstad, "On the Size of Weights for Threshold Gates", *SIAM J. on Discrete mathematics*, Vol 7, no 3, 1994, pp 484–492.

[J28] J. Håstad, A. Razborov and A. Yao, "On the Shrinkage Exponent of Read-Once Formulae", *Theoretical computer science*, 1995, Vol 141, pp 269–282.

[J29] J. Håstad, S. Jukna, and P. Pudlak "Top-Down Lower Bounds for Depth 3 Circuits", *Computational Complexity*, 1995, Vol 5, pp 99–112.

[J30] J. Håstad, T. Leighton and B. Rogoff "Analysis of Backoff Protocols for Multiple Access Channels", *SIAM Journal on Computing*, 1996, Vol 25, pp 740–774.

[J31] L. Cai, J. Chen, and J, Håstad "Circuit Bottom Fan-in and Computational Power", *SIAM Journal on Computing*, 1998, Vol 27, pp 341–355.

[J32] J. Håstad "The Shrinkage Exponent is 2", *SIAM Journal on Computing*, 1998, Vol 27, pp 48–64.

[J33] M. Goldmann and J. Håstad "Monotone Circuits for Connectivity have Depth $(\log n)^{2-o(1)}$" *SIAM Journal on Computing*, 1998, vol 27, pp 1283–1294.

[J34] M. Bellare, D. Coppersmith, J. Håstad, M. Kiwi, and M. Sudan, "Linearity Testing in Characteristic Two", *IEEE Transactions on Information Theory*, Vol 42, No 6, November 1996, pp 1781–1796.

[J35] J. Håstad, R. Impagliazzo, L. Levin, and M. Luby "A Pseudorandom Generator from any one-way function", *SIAM J. on Computing*, Vol, 28:4, 1999, pp 1364–1396. This paper was awarded SIAM Outstanding Paper Prize in 2003.

[J36] O. Goldreich, J. Håstad "On the complexity of interactive proof with bounded" communication, *Information processing letters*, Vol. 67 (4), 1998, pp 205–214.

[J37] J. Håstad "Clique is Hard to Approximate within $n^{1-\epsilon}$", *Acta Mathematica*, Vol. 182, 1999, pp 105–142.

[J38] J. Håstad "On bounded occurrence constraint satisfaction", *Information Processing Letters*, Vol. 74 (1), 2000, pp 1–6.

[J39] A. Andersson, T. Hagerup, J. Håstad, and O. Petersson, "Tight bounds for searching a sorted array of strings", *SIAM J. on Computing*, Vol 30, 2001, pp 1552-1578.

[J40] J. Håstad "Some optimal inapproximability results", *Journal of ACM*, Vol 48, 2001, pp 798-859.

[J41] G. Andersson, L. Engebretsen, and J. Håstad "A New Way to Use Semidefinite Programming with Applications to Linear Equations mod p", *Journal of Algorithms*, Vol 39, 2001, pp 162-204.

[J42] D. Dor, J. Håstad, S. Ulfberg, and U. Zwick "On lower bounds for selecting the median", *SIAM Journal on Discrete Mathematics*, Vol 14, 2001, pp 299-311.

[J43] Y. Aumann, J. Håstad, M. Rabin, and M. Sudan "Linear consistency testing", *Journal of Computer and System Sciences,* Vol 62, 2001, pp 589-607.

[J44] J. Håstad, S. Linusson and J.Wästlund "A smaller sleeping bag for a baby snake", *Discrete and Computational Geometry*, Vol 26, 2001, pp-173-181.

[J45] J. Håstad, ' A slight sharpening of LMN", *Journal of Computer and System Sciences,*, Vol 63, 2001, pp 498-508.

[J46] V. Guruswami, J. Håstad, M. Sudan and D. Zuckerman, "Combinatorial Bounds for List Decoding", *IEEE Transactions on Information Theory*, Vol 48, 2002, pp 1021-1034.

[J47] V. Guruswami, J. Håstad, and M. Sudan "Hardness of Approximate Hypergraph Coloring", *SIAM Journal on Computing*, Vol 31, 2002, pp 1663-1686.

[J48] J. Håstad, L. Ivansson, and J. Lagergren "Fitting points on the real line and its application to RH mapping", *Journal of Algorithms* Vol. 49:1, 2003, pp 42-62.

[J49] J. Håstad and A. Wigderson, "Simple Analysis of graph tests for linearity and PCP", *Random Structures and Algorithms*, Vol 22, 2003, pp 139-160.

[J50] J. Håstad and M. Näslund "The Security of all RSA and Discrete Log Bits", *Journal of the ACM*, Vol 51:2, 2004, pp 187-230.

[J51] J. Håstad and V. Srinivasan, "On the advantage over a random assignment", *Random structures and Algorithms*, Vol 25:2, 2004, pp 117-149.

[J52] J. Håstad and S. Khot, "Query efficient PCPs with perfect completeness", *Theory of Computing*, Vol 1, 2005, pp 119-149.

[J53] J. Håstad, "The square lattice shuffle", *Random structures and Algorithms*, Vol 29, 2006, pp 466-474.

[J54] J. Håstad, "The security of the IAPM and IACBC modes", *Journal of Cryptology*, Volume 20:2, 2007, pp 153-163.

[J55] J. Håstad "On the efficient approximability of constraint satisfaction problems" in Surveys in Combinatorics 2007, London Mathematical Society Lecture Notes Series, Vol 346, eds A. Hilton and J. Talbot, Cambridge University Press, 2007, pp 201-222.

[J56] J. Håstad and A. Wigderson "The randomized communicatin complexity of set disjointness" *Theory of Computing*, Vol 3, 2007, pp 211-219.

[J57] J. Håstad "Every 2-CSP Allows Nontrivial Approximation", *Computational Complexity*, Volume 17, 2008, pp 549-566.

[J58] J. Håstad and M. Näslund "Practical Construction and Analysis of Pseudorandomness Primitives", *Journal of Cryptology*, Volume 21:1, 2008, pp 1-26.

[J59] J. Håstad "On the Approximation Resistance of a Random Predicate", *Computational Complexity*, Volume 18, 2009, pp 413-434.

[J60] V. Guruswami, J. Håstad, and S. Kopparty "On the List-Decodability of Random Linear Codes", *IEEE transactions on Information Theory*, vol 57, 2011, pp 718-725.

[J61] P. Austrin and J. Håstad, "Randomly supported independence and resistance", *SIAM Journal on Computing*, volume 40, 2011, pp 1-27.

[J62] V. Guruswami, J Håstad, R. Manokaran, P. Raghavendra, and M. Charikar "Beating the Random Ordering Is Hard: Every Ordering CSP Is Approximation Resistant", *SIAM Journal on Computing*, volume 40, 2011, pp 878-914.

15 Conference Publications

[C1] J. Håstad and A. Shamir "The Cryptographic Security of Truncated Linearly related Variables" *17th Annual ACM Symposium on Theory of Computation*, 1985, pp 356–362. Later version [J4].

[C2] J. Håstad "On using RSA with Low Exponent in a Public Key Network" *Crypto 85*, 1985, pp 403–408. Later version [J5].

[C3] B. Chor, J. Friedman, O. Goldreich, J. Håstad, S. Rudich and R. Smolensky "The Bit Extraction Problem or t-resilient Functions", *Proceedings 26th Annual IEEE Symposium of Foundations of Computer Science, 1985*, pp 396–407.

[C4] J. Håstad "Almost Optimal Lower Bounds for Small Depth Circuits", *18th Annual ACM Symposium on Theory of Computation*, 1986, pp 6–20. Later version in [J9].

[C5] W. Aiello, J. Håstad and S. Goldwasser "On the Power of Interaction", *Proceedings 27th Annual IEEE Symposium of Foundations of Computer Science, 1986*, pp 368–379. Later version in [J12].

[C6] P. Beame and J. Håstad, "Optimal Bounds for Decision Problems on the CRCW PRAM", *19th Annual ACM Symposium on Theory of Computation*, 1987, pp 83–93. Later version in [J10].

[C7] J. Håstad, T. Leighton and B. Rogoff "Analysis of Backoff Protocols for Multiple Access Channels", *19th Annual ACM Symposium on Theory of Computation*, 1987, pp 241–253. Later version in [J30].

[C8] J. Håstad, T. Leighton and M. Newman "Reconfiguring a Hypercube in the Presence of Faults", *19th Annual ACM Symposium on Theory of Computation*, 1987, pp 274–284.

[C9] W. Aiello and J. Håstad "Perfect Zero-Knowledge Languages can be Recognized in Two Rounds", *Proceedings 28th Annual IEEE Symposium of Foundations of Computer Science, 1987*, pp 439–448. Later version in [J15]

[C10] J. Håstad, T. Leighton and M. Newman "Fast Computation Using Faulty Hypercubes", in proceedings of *21st Annual ACM Symposium on Theory of Computation*, 1989, pp 251–263.

[C11] M. Ben-Or, O. Goldreich, S. Goldwasser, J. Håstad, R. Impagliazzo, J. Kilian, S. Micali and P. Rogaway "Everything Provable is Provable in Zero-Knowledge", in *Crypto 88 Advances in Cryptology*, Lecture Notes in Computer Science 403, ed. S. Goldwasser, 1989, pp 37–56.

[C12] J. Håstad "Tensorrank is NP-complete", Proceedings of ICALP 1989, Lecture Notes in Computer Science, Vol 372, pp 451–460. Later version in [J11].

[C13] J. Håstad "Pseudorandom Generators under Uniform Assumptions", in proceedings of *22nd Annual ACM Symposium on Theory of Computation*, 1990, pp 395–404. Later version in [J35].

[C14] N. Alon, O. Goldreich, J. Håstad and R. Peralta."Simple Constructions of Almost k-wise Independent Random Variables", *Proceedings 31st Annual IEEE Symposium of Foundations of Computer Science, 1990*, pp 544–553. Later version in [J18].

[C15] J. Håstad and M. Goldmann "On the Power of Small-Depth Threshold Circuits",*Proceedings 31st Annual IEEE Symposium of Foundations of Computer Science, 1990*, pp 610–618. Later version in [J14].

[C16] M. Goldmann, J. Håstad and A. Razborov "Majority Gates vs. General Weighted Threshold Gates", *Proceedings 7th Structure in Complexity theory annual conference*, 1992. Later version appeared in [J17].

[C17] J. Håstad, S. Phillips and S. Safra, "A well Characterized Approximation Problem", *Israeli conference on the theory of computing and systems*, Haifa, 1993, pp 261–265. Later version appeared in [J22].

[C18] J. Håstad, S. Jukna, and P. Pudlak "Top-Down Lower Bounds for Depth 3 Circuits", *Proceedings 34th Annual IEEE Symposium of Foundations of Computer Science, 1993*, pp 124–129. Later version appeared in [J29].

[C19] J. Håstad "The Shrinkage Exponent is 2", *Proceedings 34th Annual IEEE Symposium of Foundations of Computer Science, 1993*, pp 114–123. Later version in [J32].

[C20] A. Andersson, T. Hagerup, J. Håstad and O. Petersson, "The Complexity of Searching a Sorted Array of Strings", *Proceedings of 26th Annual ACM Symposium on Theory of Computation*, 1994, pp 317–325. Later version (combined with [C22]) in [J39].

[C21] J. Håstad "Recent results in hardness of approximation", (invited presentation) *4th Scandinavian Workshop on Algorithm Theory*, 1994, pp 231–239, Springer Lecture Notes in Computer Science 824.

[C22] A. Andersson, J. Håstad and O. Petersson, "A Tight Lower Bound for Searching a Sorted Array", *Proceedings of 27th Annual ACM Symposium on Theory of Computation*, 1995, pp 417–426. Later version (combined with [C20]) in [J39].

[C23] M. Goldmann and J. Håstad "Monotone Circuits for Connectivity have Depth $(\log n)^{2-o(1)}$" *Proceedings of 27th Annual ACM Symposium on Theory of Computation*, 1995, pp 569–574. Later version in [J33].

[C24] M. Bellare, D. Coppersmith, J. Håstad, M. Kiwi, and M. Sudan, "Linearity Testing in Characteristic Two", *Proceedings 36th Annual IEEE Symposium of Foundations of Computer Science*, 1995, pp 432–441. Later version in [J34].

[C25] J. Håstad "Testing of the Long Code and Hardness for Clique" *28th Annual ACM Symposium on Theory of Computation*, 1996, pp 11–19. Complete version (combined with [C26]) in [J37].

[C26] J. Håstad "Clique is Hard to Approximate within $n^{1-\epsilon}$" *Proceedings 37th Annual IEEE Symposium of Foundations of Computer Science*, 1996, pp 627–636. Complete version (combined with [C25]) in [J37].

[C27] J. Håstad "Some Optimal In-approximability Results", *Proceedings 29th Annual ACM Symposium on Theory of Computation*, 1997, pp 1–10. Complete version appearing in [J40].

[C28] L. Cai, J. Chen, and J. Håstad "Circuit Bottom Fan-in and Computational Power", *Proceedings 12th Computational Complexity theory annual conference*, 1997. Complete version appearing in [J31].

[C29] J. Håstad "Some recent strong inapproximability results", (invited presentation) *6th Scandinavian Workshop on Algorithm Theory*, 1998, pp 205–209, Springer Lecture Notes in Computer Science 1432.

[C30] J. Håstad, L. Ivansson, and J. Lagergren "Fitting points on the real line and its application to RH mapping", *European Symposium on Algorithms*, Lecture Notes in Computer Science 1461, 1998, pp 465–476. Complete version appearing in [J48].

[C31] J. Håstad and M. Näslund "The security of individual RSA bits", *Proceedings 39th Annual IEEE Symposium on Foundations of Computer Science*, 1998, pp 510–519. Complete version appearing in [J50].

[C32] G. Andersson, L. Engebretsen, and J. Håstad "A New Way to Use Semidefinite Programming with Applications to Linear Equations mod p", *Proceedings 10th Annual ACM-SIAM Symposium on Discrete Algorithms*, 1999, pp 41–50. Complete version appearing in [J41]

[C33] Y. Aumann, J. Håstad, M. Rabin, and M. Sudan "Linear consistency testing", *Proceedings of Workshop on Randomization and Approximation Techniques in Computer Science*, Berkeley CA, August 1999. Complete version appearing in [J43].

[C34] J. Håstad "Which NP-Hard Optimization Problems Admit Non-trivial Efficient Approximation Algorithms", *Proceedings of ICALP 2000 (invited presentation)*, Lecture Notes in Computer Science, Vol 1853, pp 235–235.

[C35] V. Guruswami, J. Håstad, and M. Sudan "Hardness of Approximate Hypergraph Coloring" *Proceedings of 41st Annual IEEE Symposium on Foundations of Computer Science*, 2000, pp 149-158. Complete version appearing in [J47].

[C36] V. Guruswami, J. Håstad, M. Sudan and D. Zuckerman, "Combinatorial Bounds for List Decoding", invited paper at the *38th Annual Allerton Conference of Communication, Control and Computing*, October 2000. Complete version appearing in [J46].

[C37] J. Håstad, J. Jonsson, A. Juels, and M. Yung, "Funkspiel Schemes: An Alternative to Conventional Tamper Resistance", *Proceedings of the 7th ACM Conference on Computer Communications Security.* S. Jajodia and P. Samarati, eds. ACM Press, pp. 125-133. 2000.

[C38] J. Håstad and M. Näslund, "BMGL: Synchronous Key-stream Generator with Provable security", *Proceedings of the 1st Open NESSIE Workshop,* Nov 13-14 2000. Closely related to [C41] and complete version appearing in [J58].

[C39] J. Håstad and A. Wigderson, "Simple Analysis of graph tests for linearity and PCP", Proc. of Conference on Computational Complexity, pp. 244–255, Chicago, June 2001. Complete version appearing in [J49].

[C40] J. Håstad and S. Khot, "Query efficient PCPs with perfect completeness", Proceedings of 42nd Annual IEEE Symposium on Foundations of Computer Science, 2001, pp 610–619. Complete version appearing in [J52]

[C41] J. Håstad and M. Näslund, "Practical Construction and Analysis of Pseudo-randomness Primitives", in Colin Boyd (Ed.), Advances in Cryptology—Asiacrypt 2001, LNCS 2248, Springer-Verlag 2001, pp. 442–459. Closely related to [C38] and complete version appearing in [J58].

[C42] J. Håstad and V. Srinivasan, "On the advantage over a random assignment", Proceedings of the 34th Annual ACM Symposium on Theory of Computation, pp 43–52, Montreal, May 2002. Complete version appearing in [J51].

[C43] J. Håstad "Inapproximability-Some history and some open problems", Proceedings of the 18th Annual IEEE conference on Computational Complexity (invited presentation), pp 265-266, Aarhus, July, 2003.

[C44] Y. Dodis, R. Gennaro, J. Håstad, H. Krawczyk, and T. Rabin "Randomness Extraction and Key Derivation Using the CBC, Cascade and HMAC Modes", proceedings of CRYPTO 2004, Lecture Notes in Computer Science, vol 3152, 2004, ed M. Franklin, Springer Verlag, pp 494-510.

[C45] J. Håstad "Complexity theory, proofs and approximation", plenary address, Europeand Congress of Mathematics, editor A. Laptev, European Mathematical Society, 2005.

[C46] J. Håstad "Every 2-CSP Allows Nontrivial Approximation", Proceedings of the 37th Annual ACM Symposium on Theory of Computation, pp 740–746, Baltimore, May 2005. Complete version appearing in [J57].

[C47] J. Håstad "On Nontrivial Approximation of CSPs", abstract, invited presentation, Approximation, Randomization and Combinatorial Optimization, Proceedings of RANDOM 2006 and APPROX 2006, LNCS 4110, eds J. Diaz, K. Jansen, J. Rolim and U. Zwick, pp 1-1.

[C48] J. Håstad "On the Approximation Resistance of a Random Predicate", Approximation, Randomization and Combinatorial Optimization, Proceedings of RANDOM 2007 and APPROX 2007, LNCS 4627, eds M. Charikar, K. Jansen, Omer Reingold and J. Rolim, 2007, pp 149-163, full version appearing in [J59].

[C49] J. Nordström and J. Håstad, "Towards an Optimal Separation of Space and Length in Resolution", Proceedings of the 37th Annual ACM Symposium on Theory of Computation, pp 701–710, Victoria, British Columbia, May 2008.

[C50] P. Austrin and J. Håstad, "Randomly supported independence and resistance", 41st Annual ACM Symposium on Theory of Computation, Washington DC, pp 483-492, May 2009, full version appearing in [J61].

[C51] J. Håstad, R. Pass, D. Wikström and K. Pietrzak "An Efficient Parallel Repetition Theorem" Theory of Cryptography, Proceedins for 7th Theory of Cryptography Conference, eds. D. Micciancio, Springer Lecture Notes in Computer Science, 5978, pp 1-18, February 2010.

[C52] V. Guruswami, J. Håstad, and S. Kopparty "On the List-Decodability of Random Linear Codes", 42nd Annual ACM, Symposium on Theory of

Computation, 2010, Cambridge, MA, pp 409-416, full version appearing in [J60].

[C53] M. Cheraghchi, J. Håstad, M. Isaksson and O. Svensson, "Approximating Linear Threshold Predicates", Proceedings of APPROX 2010, Barcelona. Springer Lecture Notes in Computer Science, Vol 6302, 2010, pp 110-123.

[C54] J. Håstad, "Satisfying degree-d equations of $GF[2]^n$", Proceedings of APPROX 2011, Princeton. Springer Lecture Notes in Computer Science, Vol 6845, 2011, pp 242-253.

16 Books

[B1] J. Håstad "Computational Limitations of Small Depth Circuits", MIT PRESS, 1986.

17 Articles in popular press

[P1] J. Håstad, "Ett datornät utan chiffer är som en stad med olåsta dörrar", *Forskning och Framsteg*, Nr 8, 1995, pp 23–27 (in Swedish).