Johan HÃ¥stad

List of Publications by Year
in descending order

90 papers	6,836 citations	201674 27 h-index	82547 72 g-index
93 all docs	93 docs citations	93 times ranked	2429 citing authors

#	Article	IF	Citations
1	Explicit Two-Deletion Codes With Redundancy Matching the Existential Bound. IEEE Transactions on Information Theory, 2021, 67, 6384-6394.	2.4	20
2	Super-Polylogarithmic Hypergraph Coloring Hardness via Low-Degree Long Codes. SIAM Journal on Computing, 2017, 46, 132-159.	1.0	3
3	$(2+varepsilon)$-Sat Is NP-hard. SIAM Journal on Computing, 2017, 46, 1554-1573.	1.0	25
4	An Average-Case Depth Hierarchy Theorem for Boolean Circuits. Journal of the ACM, 2017, 64, 1-27.	2.2	11
5	On Small-Depth Frege Proofs for Tseitin for Grids. , 2017, , .		33
6	An Average-Case Depth Hierarchy Theorem for Higher Depth. , 2016, , .		3
7	Making the Long Code Shorter. SIAM Journal on Computing, 2015, 44, 1287-1324.	1.0	8
8	(2 + epsilon)-Sat Is NP-Hard. , 2014, , .		3
9	Super-polylogarithmic hypergraph coloring hardness via low-degree long codes. , 2014, , .		4
10	On the Correlation of Parity and Small-Depth Circuits. SIAM Journal on Computing, 2014, 43, 1699-1708.	1.0	31
11	On the NP-Hardness of Max-Not-2. SIAM Journal on Computing, 2014, 43, 179-193.	1.0	9
12	On DNF Approximators for Monotone Boolean Functions. Lecture Notes in Computer Science, 2014, , 235-246.	1.3	1
13	On the usefulness of predicates. ACM Transactions on Computation Theory, 2013, 5, 1-24.	0.7	13
14	On the power of many one-bit provers. , 2013, , .		1
15	Approximating Linear Threshold Predicates. ACM Transactions on Computation Theory, 2012, 4, 1-31.	0.7	4
16	Making the Long Code Shorter. , 2012, , .		28
17	On the Usefulness of Predicates. , 2012, , .		8
18	On the NP-Hardness of Max-Not-2. Lecture Notes in Computer Science, 2012, , 170-181.	1.3	3

#	Article	IF	Citations
19	Randomly Supported Independence and Resistance. SIAM Journal on Computing, 2011, 40, 1-27.	1.0	19
20	Beating the Random Ordering Is Hard: Every Ordering CSP Is Approximation Resistant. SIAM Journal on Computing, 2011, 40, 878-914.	1.0	53
21	On the List-Decodability of Random Linear Codes. IEEE Transactions on Information Theory, 2011, 57, 718-725.	2.4	26
22	Satisfying Degree-d Equations over GF[2] n. Lecture Notes in Computer Science, 2011, , 242-253.	1.3	2
23	Special Issue â€œConference on Computational Complexity 2009â€•Guest Editorâ€™s Foreword. Computational Complexity, 2010, 19, 151-152.	0.3	0
24	On the list-decodability of random linear codes. , 2010, , .		15
25	An Efficient Parallel Repetition Theorem. Lecture Notes in Computer Science, 2010, , 1-18.	1.3	26
26	Approximating Linear Threshold Predicates. Lecture Notes in Computer Science, 2010, , 110-123.	1.3	0
27	Randomly supported independence and resistance. , 2009, , .		8
28	On the Approximation Resistance of a Random Predicate. Computational Complexity, 2009, 18, 413-434.	0.3	6
29	Every 2-csp Allows Nontrivial Approximation. Computational Complexity, 2008, 17, 549-566.	0.3	14
30	Practical Construction and Analysis ofÂPseudo-Randomness Primitives. Journal of Cryptology, 2008, 21, 1-26.	2.8	0
31	Towards an optimal separation of space and length in resolution. , 2008, , .		13
32	The Security of the IAPM and IACBC Modes. Journal of Cryptology, 2007, 20, 153-163.	2.8	3
33	On the Approximation Resistance of a Random Predicate. Lecture Notes in Computer Science, 2007, , 149-163.	1.3	11
34	The square lattice shuffle. Random Structures and Algorithms, 2006, 29, 466-474.	1.1	9
35	Every 2-CSP allows nontrivial approximation. , 2005, , .		12
36	Randomness Extraction and Key Derivation Using the CBC, Cascade and HMAC Modes. Lecture Notes in Computer Science, 2004, , 494-510.	1.3	85

#	Article	IF	Citations
37	The security of all RSA and discrete log bits. Journal of the ACM, 2004, 51, 187-230.	2.2	28
38	On the advantage over a random assignment. Random Structures and Algorithms, 2004, 25, 117-149.	1.1	28
39	Fitting points on the real line and its application to RH mapping. Journal of Algorithms, 2003, 49, 42-62.	0.9	11
40	Simple analysis of graph tests for linearity and PCP. Random Structures and Algorithms, 2003, 22, 139-160.	1.1	61
41	Hardness of Approximate Hypergraph Coloring. SIAM Journal on Computing, 2002, 31, 1663-1686.	1.0	35
42	Combinatorial bounds for list decoding. IEEE Transactions on Information Theory, 2002, 48, 1021-1034.	2.4	65
43	Some optimal inapproximability results. Journal of the ACM, 2001, 48, 798-859.	2.2	1,009
44	On Lower Bounds for Selecting the Median. SIAM Journal on Discrete Mathematics, 2001, 14, 299-311.	0.8	10
45	A Smaller Sleeping Bag for a Baby Snake. Discrete and Computational Geometry, 2001, 26, 173-181.	0.6	6
46	A New Way of Using Semidefinite Programming with Applications to Linear Equations mod p. Journal of Algorithms, 2001, 39, 162-204.	0.9	25
47	Linear-Consistency Testing. Journal of Computer and System Sciences, 2001, 62, 589-607.	1.2	12
48	A Slight Sharpening of LMN. Journal of Computer and System Sciences, 2001, 63, 498-508.	1.2	11
49	On bounded occurrence constraint satisfaction. Information Processing Letters, 2000, 74, 1-6.	0.6	18
50	Tight Bounds for Searching a Sorted Array of Strings. SIAM Journal on Computing, 2000, 30, 1552-1578.	1.0	11
51	Clique is hard to approximate within n1â^'Îµ. Acta Mathematica, 1999, 182, 105-142.	3.9	776
52	A Pseudorandom Generator from any One-way Function. SIAM Journal on Computing, 1999, 28, 1364-1396.	1.0	1,090
53	On the complexity of interactive proofs with bounded communication. Information Processing Letters, 1998, 67, 205-214.	0.6	57
54	Monotone Circuits for Connectivity Have Depth (log n)2-o(1). SIAM Journal on Computing, 1998, 27, 1283-1294.	1.0	8

#	ARTICLE	IF	CITATIONS
55	Circuit Bottom Fan-in and Computational Power. SIAM Journal on Computing, 1998, 27, 341-355.	1.0	9
56	The Shrinkage Exponent of de Morgan Formulas is 2. SIAM Journal on Computing, 1998, 27, 48-64.	1.0	107
57	Some recent strong inapproximability results. Lecture Notes in Computer Science, 1998, , 205-209.	1.3	1
58	Some optimal inapproximability results. , 1997, , .		247
59	Analysis of Backoff Protocols for Multiple Access Channels. SIAM Journal on Computing, 1996, 25, 740-774.	1.0	138
60	Linearity testing in characteristic two. IEEE Transactions on Information Theory, 1996, 42, 1781-1795.	2.4	133
61	On the shrinkage exponent for read-once formulae. Theoretical Computer Science, 1995, 141, 269-282.	0.9	8
62	Top-down lower bounds for depth-three circuits. Computational Complexity, 1995, 5, 99-112.	0.3	21
63	On the Distribution of Multiplicative Translates of Sets of Residues (mod p). Journal of Number Theory, 1994, 46, 108-122.	0.4	0
64	On average time hierarchies. Information Processing Letters, 1994, 49, 15-20.	0.6	10
65	The random oracle hypothesis is false. Journal of Computer and System Sciences, 1994, 49, 24-39.	1.2	55
66	Optimal Depth, Very Small Size Circuits for Symmetrical Functions in AC0. Information and Computation, 1994, 108, 200-211.	0.7	11
67	On the Size of Weights for Threshold Gates. SIAM Journal on Discrete Mathematics, 1994, 7, 484-492.	0.8	100
68	The discrete logarithm modulo a composite hides O(n) Bits. Journal of Computer and System Sciences, 1993, 47, 376-404.	1.2	61
69	A well-characterized approximation problem. Information Processing Letters, 1993, 47, 301-305.	0.6	17
70	Simple Constructions of Almost k-wise Independent Random Variables. Random Structures and Algorithms, 1992, 3, 289-304.	1.1	382
71	Majority gates vs. general weighted threshold gates. Computational Complexity, 1992, 2, 277-300.	0.3	129
72	A simple lower bound for monotone clique using a communication game. Information Processing Letters, 1992, 41, 221-226.	0.6	25

#	Article	IF	Citations
73	Statistical zero-knowledge languages can be recognized in two rounds. Journal of Computer and System Sciences, 1991, 42, 327-345.	1.2	89
74	Relativized perfect zero knowledge is not BPP. Information and Computation, 1991, 93, 223-240.	0.7	5
75	On the power of small-depth threshold circuits. Computational Complexity, 1991, 1, 113-129.	0.3	173
76	Simultaneously good bases of a lattice and its reciprocal lattice. Mathematische Annalen, 1990, 287, 163-174.	1.4	5
77	On the power of interaction. Combinatorica, 1990, 10, 3-25.	1.2	17
78	Tensor rank is NP-complete. Journal of Algorithms, 1990, 11, 644-654.	0.9	430
79	Everything Provable is Provable in Zero-Knowledge. Lecture Notes in Computer Science, 1990, , 37-56.	1.3	103
80	Optimal bounds for decision problems on the CRCW PRAM. Journal of the ACM, 1989, 36, 643-670.	2.2	116
81	Polynomial Time Algorithms for Finding Integer Relations among Real Numbers. SIAM Journal on Computing, 1989, 18, 859-881.	1.0	84
82	Dual vectors and lower bounds for the nearest lattice point problem. Combinatorica, 1988, 8, 75-81.	1.2	25
83	Reconstructing Truncated Integer Variables Satisfying Linear Congruences. SIAM Journal on Computing, 1988, 17, 262-280.	1.0	94
84	Solving Simultaneous Modular Equations of Low Degree. SIAM Journal on Computing, 1988, 17, 336-341.	1.0	125
85	One-way permutations in NC0. Information Processing Letters, 1987, 26, 153-155.	0.6	30
86	Does co-NP have short interactive proofs?. Information Processing Letters, 1987, 25, 127-132.	0.6	290
87	Simultaneous Diophantine approximation of rationals by rationals. Journal of Number Theory, 1986, 24, 200-228.	0.4	5
88	Inapproximability - some history and some open problems. , 0, , .		0
89	On the efficient approximability of constraint satisfaction problems. , 0, , 201-222.		9
90	Complexity Theory, Proofs and Approximation. , 0, , 733-750.		1