

Johan HÅ¥stad

List of Publications by Year in descending order

Source: <https://exaly.com/author-pdf/4971208/publications.pdf>

Version: 2024-02-01

90
papers

6,836
citations

201385

27
h-index

82410

72
g-index

93
all docs

93
docs citations

93
times ranked

2429
citing authors

#	ARTICLE	IF	CITATIONS
1	A Pseudorandom Generator from any One-way Function. SIAM Journal on Computing, 1999, 28, 1364-1396.	0.8	1,090
2	Some optimal inapproximability results. Journal of the ACM, 2001, 48, 798-859.	1.8	1,009
3	Clique is hard to approximate within $n^{1-\epsilon}$. Acta Mathematica, 1999, 182, 105-142.	1.4	776
4	Tensor rank is NP-complete. Journal of Algorithms, 1990, 11, 644-654.	0.9	430
5	Simple Constructions of Almost k -wise Independent Random Variables. Random Structures and Algorithms, 1992, 3, 289-304.	0.6	382
6	Does co-NP have short interactive proofs?. Information Processing Letters, 1987, 25, 127-132.	0.4	290
7	Some optimal inapproximability results. , 1997, , .		247
8	On the power of small-depth threshold circuits. Computational Complexity, 1991, 1, 113-129.	0.2	173
9	Analysis of Backoff Protocols for Multiple Access Channels. SIAM Journal on Computing, 1996, 25, 740-774.	0.8	138
10	Linearity testing in characteristic two. IEEE Transactions on Information Theory, 1996, 42, 1781-1795.	1.5	133
11	Majority gates vs. general weighted threshold gates. Computational Complexity, 1992, 2, 277-300.	0.2	129
12	Solving Simultaneous Modular Equations of Low Degree. SIAM Journal on Computing, 1988, 17, 336-341.	0.8	125
13	Optimal bounds for decision problems on the CRCW PRAM. Journal of the ACM, 1989, 36, 643-670.	1.8	116
14	The Shrinkage Exponent of de Morgan Formulas is 2. SIAM Journal on Computing, 1998, 27, 48-64.	0.8	107
15	Everything Provable is Provable in Zero-Knowledge. Lecture Notes in Computer Science, 1990, , 37-56.	1.0	103
16	On the Size of Weights for Threshold Gates. SIAM Journal on Discrete Mathematics, 1994, 7, 484-492.	0.4	100
17	Reconstructing Truncated Integer Variables Satisfying Linear Congruences. SIAM Journal on Computing, 1988, 17, 262-280.	0.8	94
18	Statistical zero-knowledge languages can be recognized in two rounds. Journal of Computer and System Sciences, 1991, 42, 327-345.	0.9	89

#	ARTICLE	IF	CITATIONS
19	Randomness Extraction and Key Derivation Using the CBC, Cascade and HMAC Modes. Lecture Notes in Computer Science, 2004, , 494-510.	1.0	85
20	Polynomial Time Algorithms for Finding Integer Relations among Real Numbers. SIAM Journal on Computing, 1989, 18, 859-881.	0.8	84
21	Combinatorial bounds for list decoding. IEEE Transactions on Information Theory, 2002, 48, 1021-1034.	1.5	65
22	The discrete logarithm modulo a composite hides $O(n)$ Bits. Journal of Computer and System Sciences, 1993, 47, 376-404.	0.9	61
23	Simple analysis of graph tests for linearity and PCP. Random Structures and Algorithms, 2003, 22, 139-160.	0.6	61
24	On the complexity of interactive proofs with bounded communication. Information Processing Letters, 1998, 67, 205-214.	0.4	57
25	The random oracle hypothesis is false. Journal of Computer and System Sciences, 1994, 49, 24-39.	0.9	55
26	Beating the Random Ordering Is Hard: Every Ordering CSP Is Approximation Resistant. SIAM Journal on Computing, 2011, 40, 878-914.	0.8	53
27	Hardness of Approximate Hypergraph Coloring. SIAM Journal on Computing, 2002, 31, 1663-1686.	0.8	35
28	On Small-Depth Frege Proofs for Tseitin for Grids. , 2017, , .		33
29	On the Correlation of Parity and Small-Depth Circuits. SIAM Journal on Computing, 2014, 43, 1699-1708.	0.8	31
30	One-way permutations in NC0. Information Processing Letters, 1987, 26, 153-155.	0.4	30
31	The security of all RSA and discrete log bits. Journal of the ACM, 2004, 51, 187-230.	1.8	28
32	On the advantage over a random assignment. Random Structures and Algorithms, 2004, 25, 117-149.	0.6	28
33	Making the Long Code Shorter. , 2012, , .		28
34	On the List-Decodability of Random Linear Codes. IEEE Transactions on Information Theory, 2011, 57, 718-725.	1.5	26
35	An Efficient Parallel Repetition Theorem. Lecture Notes in Computer Science, 2010, , 1-18.	1.0	26
36	Dual vectors and lower bounds for the nearest lattice point problem. Combinatorica, 1988, 8, 75-81.	0.6	25

#	ARTICLE	IF	CITATIONS
37	A simple lower bound for monotone clique using a communication game. Information Processing Letters, 1992, 41, 221-226.	0.4	25
38	A New Way of Using Semidefinite Programming with Applications to Linear Equations mod p. Journal of Algorithms, 2001, 39, 162-204.	0.9	25
39	$(2+\epsilon)$ -Sat Is NP-hard. SIAM Journal on Computing, 2017, 46, 1554-1573.	0.8	25
40	Top-down lower bounds for depth-three circuits. Computational Complexity, 1995, 5, 99-112.	0.2	21
41	Explicit Two-Deletion Codes With Redundancy Matching the Existential Bound. IEEE Transactions on Information Theory, 2021, 67, 6384-6394.	1.5	20
42	Randomly Supported Independence and Resistance. SIAM Journal on Computing, 2011, 40, 1-27.	0.8	19
43	On bounded occurrence constraint satisfaction. Information Processing Letters, 2000, 74, 1-6.	0.4	18
44	On the power of interaction. Combinatorica, 1990, 10, 3-25.	0.6	17
45	A well-characterized approximation problem. Information Processing Letters, 1993, 47, 301-305.	0.4	17
46	On the list-decodability of random linear codes. , 2010, , .		15
47	Every 2-csp Allows Nontrivial Approximation. Computational Complexity, 2008, 17, 549-566.	0.2	14
48	Towards an optimal separation of space and length in resolution. , 2008, , .		13
49	On the usefulness of predicates. ACM Transactions on Computation Theory, 2013, 5, 1-24.	0.4	13
50	Linear-Consistency Testing. Journal of Computer and System Sciences, 2001, 62, 589-607.	0.9	12
51	Every 2-CSP allows nontrivial approximation. , 2005, , .		12
52	Optimal Depth, Very Small Size Circuits for Symmetrical Functions in AC0. Information and Computation, 1994, 108, 200-211.	0.5	11
53	Tight Bounds for Searching a Sorted Array of Strings. SIAM Journal on Computing, 2000, 30, 1552-1578.	0.8	11
54	A Slight Sharpening of LMN. Journal of Computer and System Sciences, 2001, 63, 498-508.	0.9	11

#	ARTICLE	IF	CITATIONS
55	Fitting points on the real line and its application to RH mapping. <i>Journal of Algorithms</i> , 2003, 49, 42-62.	0.9	11
56	An Average-Case Depth Hierarchy Theorem for Boolean Circuits. <i>Journal of the ACM</i> , 2017, 64, 1-27.	1.8	11
57	On the Approximation Resistance of a Random Predicate. <i>Lecture Notes in Computer Science</i> , 2007, , 149-163.	1.0	11
58	On average time hierarchies. <i>Information Processing Letters</i> , 1994, 49, 15-20.	0.4	10
59	On Lower Bounds for Selecting the Median. <i>SIAM Journal on Discrete Mathematics</i> , 2001, 14, 299-311.	0.4	10
60	Circuit Bottom Fan-in and Computational Power. <i>SIAM Journal on Computing</i> , 1998, 27, 341-355.	0.8	9
61	The square lattice shuffle. <i>Random Structures and Algorithms</i> , 2006, 29, 466-474.	0.6	9
62	On the efficient approximability of constraint satisfaction problems. , 0, , 201-222.		9
63	On the NP-Hardness of Max-Not-2. <i>SIAM Journal on Computing</i> , 2014, 43, 179-193.	0.8	9
64	On the shrinkage exponent for read-once formulae. <i>Theoretical Computer Science</i> , 1995, 141, 269-282.	0.5	8
65	Monotone Circuits for Connectivity Have Depth $(\log n)^{2-o(1)}$. <i>SIAM Journal on Computing</i> , 1998, 27, 1283-1294.	0.8	8
66	Randomly supported independence and resistance. , 2009, , .		8
67	On the Usefulness of Predicates. , 2012, , .		8
68	Making the Long Code Shorter. <i>SIAM Journal on Computing</i> , 2015, 44, 1287-1324.	0.8	8
69	A Smaller Sleeping Bag for a Baby Snake. <i>Discrete and Computational Geometry</i> , 2001, 26, 173-181.	0.4	6
70	On the Approximation Resistance of a Random Predicate. <i>Computational Complexity</i> , 2009, 18, 413-434.	0.2	6
71	Simultaneous Diophantine approximation of rationals by rationals. <i>Journal of Number Theory</i> , 1986, 24, 200-228.	0.2	5
72	Simultaneously good bases of a lattice and its reciprocal lattice. <i>Mathematische Annalen</i> , 1990, 287, 163-174.	0.7	5

#	ARTICLE	IF	CITATIONS
73	Relativized perfect zero knowledge is not BPP. Information and Computation, 1991, 93, 223-240.	0.5	5
74	Approximating Linear Threshold Predicates. ACM Transactions on Computation Theory, 2012, 4, 1-31.	0.4	4
75	Super-polylogarithmic hypergraph coloring hardness via low-degree long codes. , 2014, , .		4
76	The Security of the IAPM and IACBC Modes. Journal of Cryptology, 2007, 20, 153-163.	2.1	3
77	(2 + epsilon)-Sat Is NP-Hard. , 2014, , .		3
78	An Average-Case Depth Hierarchy Theorem for Higher Depth. , 2016, , .		3
79	Super-Polylogarithmic Hypergraph Coloring Hardness via Low-Degree Long Codes. SIAM Journal on Computing, 2017, 46, 132-159.	0.8	3
80	On the NP-Hardness of Max-Not-2. Lecture Notes in Computer Science, 2012, , 170-181.	1.0	3
81	Satisfying Degree-d Equations over GF[2] n. Lecture Notes in Computer Science, 2011, , 242-253.	1.0	2
82	Some recent strong inapproximability results. Lecture Notes in Computer Science, 1998, , 205-209.	1.0	1
83	On the power of many one-bit provers. , 2013, , .		1
84	On DNF Approximators for Monotone Boolean Functions. Lecture Notes in Computer Science, 2014, , 235-246.	1.0	1
85	Complexity Theory, Proofs and Approximation. , 0, , 733-750.		1
86	On the Distribution of Multiplicative Translates of Sets of Residues (mod p). Journal of Number Theory, 1994, 46, 108-122.	0.2	0
87	Inapproximability - some history and some open problems. , 0, , .		0
88	Practical Construction and Analysis of Pseudo-Randomness Primitives. Journal of Cryptology, 2008, 21, 1-26.	2.1	0
89	Special Issue "Conference on Computational Complexity 2009" Guest Editor's Foreword. Computational Complexity, 2010, 19, 151-152.	0.2	0
90	Approximating Linear Threshold Predicates. Lecture Notes in Computer Science, 2010, , 110-123.	1.0	0