Shachar Lovett

List of Publications by Year
in descending order

80 papers	948 citations	759055 12 h-index	839398 18 g-index
81 all docs	81 docs citations	81 times ranked	333 citing authors

#	Article	IF	Citations
1	On cryptography with auxiliary input. , 2009, , .		134
2	Subspace evasive sets. , 2012, , .		33
3	Worst Case to Average Case Reductions for Polynomials. , 2008, , .		30
4	Constructive Discrepancy Minimization by Walking on the Edges. , 2012, , .		30
5	Communication is bounded by root of rank. , 2014, , .		30
6	Weight Distribution and List-Decoding Size of Reedâ€"Muller Codes. IEEE Transactions on Information Theory, 2012, 58, 2689-2696.	1.5	29
7	Rectangles Are Nonnegative Juntas. SIAM Journal on Computing, 2016, 45, 1835-1869.	0.8	29
8	Constructive Discrepancy Minimization by Walking on the Edges. SIAM Journal on Computing, 2015, 44, 1573-1582.	0.8	27
9	Algebraic attacks against random local functions and their countermeasures. , 2016, , .		26
10	Inverse conjecture for the gowers norm is false. , 2008, , .		25
11	Title is missing!. Theory of Computing, 2009, 5, 69-82.	0.3	21
12	Unconditional pseudorandom generators for low degree polynomials. , 2008, , .		19
13	Nontrivial t-designs over finite fields exist for all t. Journal of Combinatorial Theory - Series A, 2014, 127, 149-160.	0.5	18
14	A tail bound for readâ€‹*k*</i> families of functions. Random Structures and Algorithms, 2015, 47, 99-108.	0.6	18
15	Rectangles Are Nonnegative Juntas. , 2015, , .		18
16	Pseudorandom Bit Generators That Fool Modular Sums. Lecture Notes in Computer Science, 2009, , 615-630.	1.0	18
17	Structure of Protocols for XOR Functions. SIAM Journal on Computing, 2018, 47, 208-217.	0.8	17
18	A Lower Bound for Dynamic Approximate Membership Data Structures. , 2010, , .		16

#	ARTICLE	IF	CITATIONS
19	Every locally characterized affine-invariant property is testable. , 2013, , .		16
20	A counterexample to a strong variant of the Polynomial Freiman-Ruzsa conjecture in Euclidean space. Discrete Analysis, 2018, , .	2.8	16
21	MDS Matrices over Small Fields: A Proof of the GM-MDS Conjecture. , 2018, , .		15
22	Communication is Bounded by Root of Rank. Journal of the ACM, 2016, 63, 1-9.	1.8	15
23	Bounded-Depth Circuits Cannot Sample Good Codes. Computational Complexity, 2012, 21, 245-266.	0.2	13
24	Near-optimal Linear Decision Trees for k-SUM and Related Problems. Journal of the ACM, 2019, 66, 1-18.	1.8	13
25	New Extension of the Weil Bound for Character Sums with Applications to Coding. , 2011, , .		12
26	Bounded-Depth Circuits Cannot Sample Good Codes. , 2011, , .		12
27	Probabilistic existence of regular combinatorial structures. Geometric and Functional Analysis, 2017, 27, 919-972.	0.6	12
28	Active Classification with Comparison Queries. , 2017, , .		12
29	Algebraic Attacks against Random Local Functions and Their Countermeasures. SIAM Journal on Computing, 2018, 47, 52-79.	0.8	11
30	Non-Malleable Codes from Additive Combinatorics. SIAM Journal on Computing, 2018, 47, 524-546.	0.8	11
31	Higher-Order Fourier Analysis Of $${\mathbb{F}_{p}^n}$$ And The Complexity Of Systems Of Linear Forms. Geometric and Functional Analysis, 2011, 21, 1331-1357.	0.6	10
32	New bounds for matching vector families. , 2013, , .		10
33	The Gram-Schmidt walk: a cure for the Banaszczyk blues. , 2018, , .		10
34	Equivalence of polynomial conjectures in additive combinatorics. Combinatorica, 2012, 32, 607-618.	0.6	9
35	An Additive Combinatorics Approach Relating Rank to Communication Complexity. , 2012, , .		8
36	General systems of linear forms: Equidistribution and true complexity. Advances in Mathematics, 2016, 292, 446-477.	0.5	8

#	ARTICLE	IF	CITATIONS
37	Structure of Protocols for XOR Functions. , 2016, , .		8
38	Testing Low Complexity Affine-Invariant Properties. , 2013, , .		8
39	Probabilistic existence of rigid combinatorial structures. , 2012, , .		7
40	Variety Evasive Sets. Computational Complexity, 2014, 23, 509-529.	0.2	7
41	New Bounds for Matching Vector Families. SIAM Journal on Computing, 2014, 43, 1654-1683.	0.8	7
42	Near-optimal linear decision trees for k-SUM and related problems. , 2018, , .		7
43	ALMOST EUCLIDEAN SECTIONS OF THE N-DIMENSIONAL CROSS-POLYTOPE USING O(N) RANDOM BITS. Communications in Contemporary Mathematics, 2008, 10, 477-489.	0.6	6
44	The Complexity of Boolean Functions in Different Characteristics. Computational Complexity, 2010, 19, 235-263.	0.2	6
45	Random low-degree polynomials are hard to approximate. Computational Complexity, 2012, 21, 63-81.	0.2	6
46	Estimating the Distance from Testable Affine-Invariant Properties. , 2013, , .		6
47	Almost K-Wise vs. K-Wise Independent Permutations, and Uniformity for General Group Actions. Lecture Notes in Computer Science, 2012, , 350-361.	1.0	6
48	Large Deviation Bounds for Decision Trees and Sampling Lower Bounds for AC0-Circuits. , 2012, , .		5
49	An Additive Combinatorics Approach Relating Rank to Communication Complexity. Journal of the ACM, 2014, 61, 1-18.	1.8	5
50	The Freimanâ€"Ruzsa theorem over finite fields. Journal of Combinatorial Theory - Series A, 2014, 125, 333-341.	0.5	5
51	Improved Noisy Population Recovery, and Reverse Bonami-Beckner Inequality for Sparse Functions. , 2015, , .		5
52	The Independence Number of the Birkhoff Polytope Graph, and Applications to Maximally Recoverable Codes. , 2017, , .		5
53	The List Decoding Radius for Reedâ€"Muller Codes Over Small Fields. IEEE Transactions on Information Theory, 2018, 64, 4382-4391.	1.5	5
54	Log-rank and lifting for AND-functions. , 2021, , .		5

#	Article	IF	Citations
55	Correlation testing for affine invariant properties on Fpnin the high error regime. , 2011, , .		4
56	The List Decoding Radius of Reed-Muller Codes over Small Fields. , 2015, , .		4
57	Affine-malleable extractors, spectrum doubling, and application to privacy amplification. , 2016, , .		4
58	An improved lower bound for arithmetic regularity. Mathematical Proceedings of the Cambridge Philosophical Society, 2016, 161, 193-197.	0.3	4
59	Title is missing!. Theory of Computing, 2011, 7, 185-188.	0.3	4
60	Correlation Bounds for Poly-size $\mbox{m AC}^0$ Circuits with n 1â€‰â‹â€‰o(1) Symmetric Gates. Lecture Notes in Computer Science, 2011, , 640-651.	1.0	4
61	On the Complexity of Boolean Functions in Different Characteristics. , 2009, , .		3
62	Pseudorandom Generators for CC0[p] and the Fourier Spectrum of Low-Degree Polynomials over Finite Fields. , 2010, , .		3
63	Linear Systems over Finite Abelian Groups. , 2011, , .		3
64	Pseudorandom generators for CC0[p] and the Fourier spectrum of low-degree polynomials over finite fields. Computational Complexity, 2013, 22, 679-725.	0.2	3
65	On the Impossibility of Entropy Reversal, and Its Application to Zero-Knowledge Proofs. Lecture Notes in Computer Science, 2017, , 31-55.	1.0	3
66	Higher-order Fourier Analysis and Applications. Foundations and Trends in Theoretical Computer Science, 2019, 13, 247-448.	2.0	3
67	The Independence Number of the Birkhoff Polytope Graph, and Applications to Maximally Recoverable Codes. SIAM Journal on Computing, 2019, 48, 1425-1435.	0.8	3
68	On the Beckâ€Fiala conjecture for random set systems. Random Structures and Algorithms, 2019, 54, 665-675.	0.6	3
69	XOR lemmas for resilient functions against polynomials. , 2020, , .		3
70	A Space Lower Bound for Dynamic Approximate Membership Data Structures. SIAM Journal on Computing, 2013, 42, 2182-2196.	0.8	2
71	Random Low Degree Polynomials are Hard to Approximate. Lecture Notes in Computer Science, 2009, , 366-377.	1.0	2
72	Probabilistic Existence of Large Sets of Designs. , 2018, , 1545-1556.		2

#	Article	IF	Citations
73	Holes in Generalized Reedâ€"Muller Codes. IEEE Transactions on Information Theory, 2010, 56, 2583-2586.	1.5	1
74	Correlation Testing for Affine Invariant Properties on $\mathbb{F}_p^n$ in the High Error Regime. SIAM Journal on Computing, 2014, 43, 1417-1455.	0.8	1
75	Group representations that resist random sampling. Random Structures and Algorithms, 2015, 47, 605-614.	0.6	1
76	Sparse MDS Matrices over Small Fields: A Proof of the GM-MDS Conjecture. SIAM Journal on Computing, 2021, 50, 1248-1262.	0.8	1
77	Point Location and Active Learning: Learning Halfspaces Almost Optimally. , 2020, , .		1
78	Pseudorandom Generators for Read-Once ACC^0. , 2012, , .		0
79	On the structure of the spectrum of small sets. Journal of Combinatorial Theory - Series A, 2017, 148, 1-14.	0.5	0
80	The Robust Sensitivity of Boolean Functions. , 2018, , 1822-1833.		0