---

**Zbl 1172.68045**

**Elkin, Michael; Emek, Yuval; Spielman, Daniel A.; Teng, Shang-Hua**

**Lower-stretch spanning trees.** (English)

SIAM J. Comput. 38, No. 2, 608-628 (2008). ISSN 0097-5397; ISSN 1095-7111
http://dx.doi.org/10.1137/050641661
http://epubs.siam.org/sam-bin/dbq/toclist/SICOMP

Summary: We show that every weighted connected graph $G$ contains as a subgraph a spanning tree into which the edges of $G$ can be embedded with average stretch $O(\log^2 n \log\log n)$. Moreover, we show that this tree can be constructed in time $O(m \log n + n \log^2 n)$ in general, and in time $O(m \log n)$ if the input graph is unweighted. The main ingredient in our construction is a novel graph decomposition technique. Our new algorithm can be immediately used to improve the running time of the recent solver for symmetric diagonally dominant linear systems of Spielman and Teng from $m2^{(O(\sqrt{\log n \log\log n}))}$ to $m \log^{O(1)} n$, and to $O(n \log^2 n \log\log n)$ when the system is planar. Our result can also be used to improve several earlier approximation algorithms that use low-stretch spanning trees.

*Keywords* : low-distortion embeddings; probabilistic tree metrics; low-stretch spanning trees

*Classification* :

∗68R10 Graph theory in connection with computer science
05C85 Graphic algorithms
68Q25 Analysis of algorithms and problem complexity

---

**Zbl pre05485569**

**Spielman, Daniel A.; Srivastava, Nikhil**

**Graph sparsification by effective resistances.** (English)

STOC'08. Proceedings of the 40th annual ACM symposium on theory of computing 2008, Victoria, Canada, May 17–20, 2008.. 563-568 (2008). ISBN 978-1-60558-047-0

*Classification* :

∗68R10 Graph theory in connection with computer science
65W05

---

**Zbl pre05485557**

**Daitch, Samuel I.; Spielman, Daniel A.**

**Faster approximate lossy generalized flow via interior point algorlthms.** (English)

STOC'08. Proceedings of the 40th annual ACM symposium on theory of computing 2008, Victoria, Canada, May 17–20, 2008.. 451-460 (2008). ISBN 978-1-60558-047-0

*Classification* :
∗68W25 Approximation algorithms

---

**Zbl 1122.05062**

**Spielman, Daniel A.; Teng, Shang-Hua**

**Spectral partitioning works: planar graphs and finite element meshes.** (English)

Linear Algebra Appl. 421, No. 2-3, 284-305 (2007). ISSN 0024-3795
http://dx.doi.org/10.1016/j.laa.2006.07.020
http://www.sciencedirect.com/science/journal/00243795
http://www.elsevier.com/locate/issn/0024-3795

Summary: Spectral partitioning methods use the Fiedler vector – the eigenvector of the second-smallest eigenvalue of the Laplacian matrix – to find a small separator of a graph. These methods are important components of many scientific numerical algorithms and have been demonstrated by experiment to work extremely well. In this paper, we show that spectral partitioning methods work well on bounded-degree planar graphs and finite element meshes – the classes of graphs to which they are usually applied. While naive spectral bisection does not necessarily work, we prove that spectral partitioning techniques can be used to produce separators whose ratio of vertices removed to edges cut is $O(\sqrt{n})$ for bounded-degree planar graphs and two-dimensional meshes and $O(n^{1/d})$ for well-shaped $d$-dimensional meshes. The heart of our analysis is an upper bound on the second-smallest eigenvalues of the Laplacian matrices of these graphs: we prove a bound of $O(1/n)$ for bounded-degree planar graphs and $O(1/n^{2/d})$ for well-shaped $d$-dimensional meshes.

*Keywords* : spectral methods; spectral analysis; graph partitioning; eigenvalue problems; graph embedding
*Classification* :
∗05C50 Graphs and matrices
05C10 Topological graph theory

---

**Zbl 1114.65024**

**Spielman, Daniel A.; Teng, Shang-Hua; Üngör, Alper**

**Parallel Delaunay refinement: algorithms and analyses.** (English)

Int. J. Comput. Geom. Appl. 17, No. 1, 1-30 (2007). ISSN 0218-1959
http://dx.doi.org/10.1142/S0218195907002227
http://www.worldscinet.com/ijcga/ijcga.shtml

Summary: The authors present a parallel Delaunay refinement algorithm for generating well-shaped meshes in both two and three dimensions. Like its sequential counterparts, the parallel algorithm iteratively improves the quality of a mesh by inserting new points, the Steiner points, into the input domain while maintaining the Delaunay triangulation.

The Steiner points are carefully chosen from a set of candidates that includes the circumcenters of poorly-shaped triangular elements. They introduce a notion of independence among possible Steiner points that can be inserted simultaneously during Delaunay refinements and show that such a set of independent points can be constructed efficiently and that the number of parallel iterations is $O(\log^2 \Delta)$, where $\Delta$ is the spread of the input – the ratio of the longest to the shortest pairwise distances among input features. In addition, they show that the parallel insertion of these set of points can be realized by sequential Delaunay refinement algorithms such as by Ruppert's algorithm in two dimensions and Shewchuk's algorithm in three dimensions. Therefore, his parallel Delaunay refinement algorithm provides the same shape quality and mesh-size guarantees as these sequential algorithms. For generating quasi-uniform meshes, such as those produced by Chew's algorithms, the number of parallel iterations is in fact $O(\log \Delta)$. To the best of my knowledge and of the authors', this algorithm is the first provably polylog($\Delta$) time parallel Delaunay-refinement algorithm that generates well-shaped meshes of size within a constant factor of the best possible.

*Keywords* : simplicial meshes; parallel algorithms; computational geometry
*Classification* :
∗65D18 Computer graphics and computational geometry

---

**Zbl 1179.65033**

**Sankar, Arvind; Spielman, Daniel A.; Teng, Shang-Hua**

**Smoothed analysis of the condition numbers and growth factors of matrices.**

(English)
SIAM J. Matrix Anal. Appl. 28, No. 2, 446-476 (2006). ISSN 0895-4798; ISSN 1095-7162
http://dx.doi.org/10.1137/S0895479803436202
http://epubs.siam.org/sam-bin/dbq/toclist/SIMAX

Summary: Let $\bar{A}$ be an arbitrary matrix and let $A$ be a slight random perturbation of $\bar{A}$. We prove that it is unlikely that $A$ has a large condition number. Using this result, we prove that it is unlikely that $A$ has large growth factor under Gaussian elimination without pivoting. By combining these results, we show that the smoothed precision necessary to solve $Ax = b$, for any $b$, using Gaussian elimination without pivoting is logarithmic. Moreover, when $\bar{A}$ is an all-zero square matrix, our results significantly improve the average-case analysis of Gaussian elimination without pivoting performed by *M.-C. Yeung* and *T. F. C. Chan* [SIAM J. Matrix Anal. Appl. 18, No. 2, 499–517 (1997; Zbl 0871.65019)]."

*Keywords* : smoothed analysis; condition number; Gaussian elimination; growth factor
*Classification* :
∗65F05 Direct methods for linear systems
15A12 Conditioning of matrices
65F35 Matrix norms, etc. (numerical linear algebra)

---

**Zbl 1122.68300**

**STOC '06: Proceedings of the 38th annual ACM symposium on theory of computing, Seattle, WA, USA, May 21–23, 2006.** (English)

New York, NY: ACM Press. xiv, 768 p. (2006). ISBN 1-59593-134-1

Contents: Venkatesan Guruswami and Atri Rudra, Explicit capacity-achieving list-decodable codes or decoding up to the singleton bound using folded Reed-Solomon codes (1–10); Alex Samorodnitsky and Luca Trevisan, Gowers uniformity, influence of variables, and PCPs (11–20); Dana Moshkovitz and Ran Raz, Sub-constant error low degree test of almost-linear size (21–30); Nikhil Bansal and Maxim Sviridenko, The Santa Claus problem (31–40); Uriel Feige, On maximizing welfare when utility functions are subadditive (41–50); Jonathan A. Kelner and Daniel A. Spielman, A randomized polynomial-time simplex algorithm for linear programming (51–60); Paul W. Goldberg and Christos H. Papadimitriou, Reducibility among equilibrium problems (61–70); Constantinos Daskalakis, Paul W. Goldberg and Christos H. Papadimitriou, The complexity of computing a Nash equilibrium (71–78); Tim Roughgarden and Mukund Sundararajan, New trade-offs in cost-sharing mechanisms (79–88); Ara Hayrapetyan, Éva Tardos and Tom Wexler, The effect of collusion in congestion games (extended abstract) (89–98).

Yuval Ishai, Eyal Kushilevitz, Yehuda Lindell and Erez Petrank, Black-box constructions for secure computation (extended abstract) (99–108); Eyal Kushilevitz, Yehuda Lindell and Tal Rabin, Information-theoretically secure protocols and security under composition (109–118); Amos Beimel, Paz Carmi, Kobbi Nissim and Enav Weinreb, Private approximation of search problems (119–128); Prabhakar Raghavan, The changing face of web search: algorithms, auctions and advertising (129); Dimitris Achlioptas and Federico Ricci-Tersenghi, On the solution-space geometry of random constraint satisfaction problems (130–139) Dror Weitz, Counting independent sets up to the tree threshold (140–149); Mario Szegedy, The DLT priority sampling is essentially optimal (extended abstract) (150–158; Constantinos Daskalakis, Elchanan Mossel and Sébastien Roch, Optimal phylogenetic reconstruction (159–168); Panagiota Fatourou, Faith Ellen Fich and Eric Ruppert, Time-space tradeoffs for implementations of snapshots (169–178); Michael Ben-Or, Elan Pavlov and Vinod Vaikuntanathan, Byzantine agreement in the full-information model in $O(\log n)$ rounds (179–186).

Spyridon Antonakopoulos, Fast leader-election protocols with bounded cheaters' edge (187–196); Sung-woo Cho and Ashish Goel, Pricing for fairness: distributed resource allocation for multiple objectives (197–204); Moses Charikar, Konstantin Makarychev and Yury Makarychev, Near-optimal algorithms for unique games (extended abstract) (205–214); Sanjeev Arora, Eden Chlamtac and Moses Charikar, New approximation guarantee for chromatic number (215–224); Virginia Vassilevska and Ryan Williams, Finding a maximum weight triangle in $n^{3-\delta}$ time, with applications (225–231); Mihai Pătraşcu and Mikkel Thorup, Time-space trade-offs for predecessor search (extended abstract) (232–240); Irit Dinur, The PCP theorem by gap amplification (extended abstract) (241–250); Noga Alon, Eldar Fischer, Ilan Newman and Asaf Shapira, A combinatorial characterization of the testable graph properties: it's all about regularity (251–260); Christian Borgs, Jennifer Chayes, László Lovász, Vera T. Sós, Balázs Szegedy

and Katalin Vesztergombi, Graph limits and parameter testing (261–270); Ittai Abraham, Yair Bartal and Ofer Neiman, Advances in metric embedding theory (extended abstract) (271–286).

Minh-Huyen Nguyen and Salil Vadhan, Zero knowledge with efficient provers (287–295); John Watrous, Zero-knowledge against quantum attacks (296–305); Silvio Micali and Rafael Pass, Local zero knowledge (306–315); Jan Remy and Angelika Steger, A quasi-polynomial time approximation scheme for minimum weight triangulation (extended abstract) (316–325); Kenneth L. Clarkson, Building triangulations using $\epsilon$-nets (extended abstract) (326–335); Tetsuo Asano, Jiří Matoušek and Takeshi Tokuyama, The distance trisector curve (336–343); Irit Dinur, Elchanan Mossel and Oded Regev, Conditional hardness for approximate coloring (344–353); Michael R. Fellows, Frances A. Rosamond, Udi Rotics and Stefan Szeider, Clique-width minimization is NP-hard (extended abstract) (354–362); Vitaly Feldman, Hardness of approximate two-level logic minimization and PAC learning with membership queries (363–374); Russell Impagliazzo, Can every randomized algorithm be derandomized? (373–374).

Uriel Feige and Mohammad Mahdian, Finding small balanced separators (375–384); Rohit Khandekar, Satish Rao and Umesh Vazirani, Graph partitioning using single commodity flows (385–390); Jaroslav Nešetřil and Patrice Ossona de Mendez, Linear time low tree-width partitions and algorithmic consequences (391–400); Ken-ichi Kawarabayashi and Bojan Mohar, Approximating the list-chromatic number and the chromatic number in minor-closed and odd-minor-closed classes of graphs (401–416); Leonid Gurvits, Hyperbolic polynomials approach to Van der Waerden/Schrijver-Valiant like conjectures: sharper bounds, simpler proofs and algorithmic applications (417–426); Dorit Aharonov, Vaughan Jones and Zeph Landau, A polynomial quantum algorithm for approximating the Jones polynomial (427–436); Irit Dinur, Ehud Friedgut, Guy Kindler and Ryan O'Donnell, On the Fourier tails of bounded functions over the discrete cube (extended abstract) (437–446); Oded Regev and Ricky Rosen, Lattice problems and norm embeddings (447–456); Omer Reingold, Luca Trevisan and Salil Vadhan, Pseudorandom walks on regular digraphs and the $RL$ vs. $L$ problem (457–466); Wojciech Plandowski, An efficient algorithm for solving word equations (extended abstract) (467–476).

Peter DeMarzo, Ilan Kremer and Yishay Mansour, Online trading algorithms and robust option pricing (477–486); Konstantinos Panagiotou and Alexander Souza, On adequate performance measures for paging (487–496); Anup Rao, Extractors for a constant number of polynomially small min-entropy independent sources (497–506); Jakob Nordström, Narrow proofs may be spacious: separating space and width in resolution (extended abstract) (507–516) Matthew Andrews and Lisa Zhang, Logarithmic hardness of the directed congestion minimization problem (517–526); Julia Chuzhoy and Sanjeev Khanna, Hardness of cut problems in directed graphs (extended abstract) (527–536) Nikhil R. Devanur, Subhash A. Khot, Rishi Saket and Nisheeth K. Vishnoi, Integrality gaps for sparsest cut and minimum linear arrangement problems (537–546); Howard Karloff, Subhash Khot, Aranyak Mehta and Yuval Rabani, On earthmover distance, metric labelling, and 0-extension (547–556); Nir Ailon and Bernard Chazelle, Approximate nearest neighbors and the fast Johnson-Lindenstrauss transform (557–563); Sunil Arya, Theocharis Malamatos and David M. Mount, On the importance of idempotence (564–573).

Richard Cole and Lee-Ad Gottlieb, Searching dynamic point sets in spaces with bounded doubling dimension (574–583); Dana Angluin, James Aspnes, Jiang Chen and Yinghua Wu, Learning a circuit by injecting values (extended abstract) (584–593); Dmitry Gavinsky, Julia Kempe, Oded Regev and Ronald de Wolf, Bounded-error quantum state identification and exponential separations in communication complexity (594–603); Sean Hallgren, Cristopher Moore, Martin Rötteler, Alexander Russell and Pranab Sen, Limitations of quantum coset states for graph isomorphism (604–617); Andris Ambainis, Robert Špalek and Ronald de Wolf, A new quantum lower bound method, with applications to direct product theorems and time-space tradeoffs (618–633) Shengyu Zhang, New upper and lower bounds for randomized and quantum local search (634–643) Shahar Dobzinski, Noam Nisan and Michael Schapira, Truthful randomized mechanisms for combinatorial auctions (644–652)Simon Fischer, Harald Räcke and Berthold Vöcking, Fast convergence to Wardrop equilibria by adaptive sampling methods (653–662)Lisa Fleischer, Jochen Könemann, Stefano Leonardi and Guido Schäfer, Simple cost sharing schemes for multicommodity rent-or-buy and stochastic Steiner tree (663–670); Boaz Barak, Anup Rao, Ronen Shaltiel and Avi Wigderson, 2-source dispersers for sub-polynomial entropy and Ramsey graphs beating the Frankl-Wilson construction (671–680).
David Zuckerman, Linear degree extractors and the inapproximability of max clique and chromatic number (681–690); Jesse Kamp, Anup Rao, Salil Vadhan and David Zuckerman, Deterministic extractors for small-space sources (691–700); Adi Akavia, Oded Goldreich, Shafi Goldwasser and Dana Moshkovitz, On basing one-way functions on NP-hardness (701–710) ; Bella Dubrov and Yuval Ishai, On the randomness complexity of efficient sampling (extended abstract) (711–720) Nikhil Bansal, Amit Chakrabarti, Amir Epstein and Baruch Schieber, A quasi-PTAS for unsplittable flow on line graphs (721–729); Naveen Garg and Amit Kumar, Minimizing average flow time on related machines (730–738); Retsef Levi, Robin O. Roundy and David B. Shmoys, Provably near-optimal sampling-based algorithms for stochastic inventory control models (extended abstract) (739–748); Philip N. Klein, A subset spanner for planar graphs, with application to subset TSP (749–756); Chandra Chekuri, Sanjeev Khanna and F. Bruce Shepherd, Edge-disjoint paths in planar graphs with constant congestion (757–766) .
The articles of this volume will not be reviewed individually. The preceding conference has been reviewed (see Zbl 1088.68501).

*Classification* :

∗68-06 Proceedings of conferences (computer science)
00B25 Proceedings of conferences of miscellaneous specific interest
68M10 Computer networks
68W05 Nonnumerical algorithms
68R10 Graph theory in connection with computer science

---

**Zbl 1116.68117**

**Spielman, Daniel A.; Teng, Shang-Hua**

**Smoothed analysis of algorithms and heuristics: progress and open questions.** (English)

Pardo, Luis M. (ed.) et al., Foundations of computational mathematics, Santander

2005. Selected papers based on the presentations at the international conference of the Foundations of Computational Mathematics (FoCM), Santander, Spain, June 30 – July 9, 2005. Cambridge: Cambridge University Press. London Mathematical Society Lecture Note Series 331, 274-342 (2006). ISBN 0-521-68161-8/pbk

Summary: We survey some recent progress in the smoothed analysis of algorithms and heuristics in mathematical programming, combinatorial optimization, computational geometry, and scientific computing. Our focus will be more on problems and results rather than on proofs. We discuss several perturbation models used in smoothed analysis for both continuous and discrete inputs. Perhaps more importantly, we present a collection of emerging open questions as food for thought in this field.

*Classification* :
∗68W40 Analysis of algorithms

---

**Zbl 1122.68750**

**Spielman, Daniel A.**
**The smoothed analysis of algorithms.** (English)
Liśkiewicz, Maciej (ed.) et al., Fundamentals of computation theory. 15th international symposium, FCT 2005, Lübeck, Germany, August 17–20, 2005. Proceedings. Berlin: Springer. Lecture Notes in Computer Science 3623, 17-18 (2005). ISBN 3-540-28193-2/pbk
http://dx.doi.org/10.1007/11537311

Summary: We survey the progress that has been made in the smoothed analysis of algorithms.

*Classification* :
∗68W40 Analysis of algorithms

---

**Zbl 1088.68501**

**STOC'05: Proceedings of the 37th annual ACM symposium on theory of computing, Baltimore, MD, USA, May 22–24, 2005.** (English)
New York, NY: Association for Computing Machinery (ACM). xiv, 763 p. (2005). ISBN 1-58113-960-8

Contents: Boaz Barak, Guy Kindler, Ronen Shaltiel, Benny Sudakov and Avi Wigderson, Simulating independence: new constructions of condensers, Ramsey graphs, dispersers, and extractors (1–10); Ran Raz, Extractors with weak random seeds (11–20); Andrej Bogdanov, Pseudorandom generators for low degree polynomials (21–30); Luca Trevisan, On uniform amplification of hardness in NP (31–38); Patrick Briest, Piotr Krysta and Berthold Vöcking, Approximation techniques for utilitarian mechanism design (39–48); Christos H. Papadimitriou, Computing correlated equilibria in multiplayer games (49–56) ; Baruch Awerbuch, Yossi Azar and Amir Epstein, The price of routing unsplittable flow (57–66); George Christodoulou and Elias Koutsoupias, The

price of anarchy of finite congestion games (67–73); Bruno Codenotti, Benton McCune and Kasturi Varadarajan, Market equilibrium via the excess demand function (74–83); Oded Regev, On lattices, learning with errors, random linear codes, and cryptography (84–93).

Miklós Ajtai, Representing hard lattices with $O(n \log n)$ bits (extended abstract) (94–103); Christian Worm Mortensen, Rasmus Pagh and Mihai Pătraşcu, On dynamic range reporting in one dimension (extended abstract) (104–111); Mikkel Thorup, Worst-case update times for fully-dynamic all-pairs shortest paths (112–119); Lance Fortnow, Beyond NP: the work and legacy of Larry Stockmeyer (120–127); Noga Alon and Asaf Shapira, Every monotone graph property is testable (128–137); Eldar Fischer and Ilan Newman, Testing versus estimation of graph properties (extended abstract) (138–146); Ronitt Rubinfeld and Rocco A. Servedio, Testing monotone high-dimensional distributions (147–156); Katalin Friedl, Gábor Ivanyos and Miklos Santha, Efficient testing of groups (157–166); Joseph Cheriyan and Adrian Vetta, Approximation algorithms for network design with metric costs (167–175); Moses Charikar and Adriana Karagiozova, On non-uniform multicommodity buy-at-bulk network design (176–182).

Chandra Chekuri, Sanjeev Khanna and F. Bruce Shepherd, Multicommodity flow, well-linked terminals, and routing problems (183–192); Mohammad Taghi Hajiaghayi, Jeong Han Kim, Tom Leighton and Harald Räcke, Oblivious routing in directed graphs with random demands (193–201); Piotr Indyk and David Woodruff, Optimal approximations of the frequency moments of data streams (202–208); Gereon Frahling and Christian Sohler, Coresets in dynamic geometric data streams (209–217); Rafail Ostrovsky and Yuval Rabani, Low distortion embeddings for edit distance (218–224); Mihai Bădoiu, Julia Chuzhoy, Piotr Indyk and Anastasios Sidiropoulos, Low-distortion embeddings of general metrics into the line (225–233); Mikolaj Bojanczyk and Thomas Colcombet, Tree-walking automata do not recognize all regular languages (234–243); Itai Benjamini, Oded Schramm and David B. Wilson, Balanced Boolean functions that can be evaluated so that every input bit is unlikely to be read (244–250); Michael Alekhnovich, Lower bounds for $k$-DNF resolution on random 3-CNFs (extended abstract) (251–256); Michal Koucký, Pavel Pudlák and Denis Thérien, Bounded-depth circuits: separating wires from gates (extended abstract) (257–265).

Eli Ben-Sasson and Madhu Sudan, Simple PCPs with poly-log rate and query complexity (266–275); Matthew Andrews and Lisa Zhang, Hardness of the undirected edge-disjoint paths problem (276–283); Matthew Andrews and Lisa Zhang, Hardness of the undirected congestion minimization problem (284–293); Mikhail Alekhnovich, Sanjeev Arora and Iannis Tourlakis, Towards strong nonapproximability results in the Lovasz-Schrijver hierarchy (294–303); Saugata Basu, Richard Pollack and Marie-Francoise Roy, Computing the first Betti number and the connected components of semi-algebraic sets (304–312); Saugata Basu, Polynomial time algorithm for computing the top Betti numbers of semi-algebraic sets defined by quadratic inequalities (313–322); Xi Chen and Xiaotie Deng, On algorithms for discrete and approximate Brouwer fixed points (extended abstract) (323–330); Yossi Azar and Amir Epstein, Convex programming for scheduling unrelated parallel machines (331–337); Saurabh Sanghvi and Salil Vadhan, The round complexity of two-party random selection (338–347); Lance Fortnow, Rahul Santhanam and Luca Trevisan, Hierarchies for semantic classes (extended abstract) (348–355).

Haim Kaplan, Eyal Kushilevitz and Yishay Mansour, Learning with attribute costs (356–365); Elchanan Mossel and Sébastien Roch, Learning nonsingular phylogenies and hidden Markov models (366–375); Omer Reingold, Undirected ST-connectivity in log-space (376–385); Lujun Jia, Guolong Lin, Guevara Noubir, Rajmohan Rajaraman and Ravi Sundaram, Universal approximations for TSP, Steiner tree, and set cover (386–395); Naveen Garg, Saving an epsilon: a 2-approximation for the $k$-MST problem in graphs (396–402); Ben Morris, The mixing time of the Thorp shuffle (403–412); Mary Cryan, Martin Dyer and Dana Randall, Approximately counting integral flows and cell-bounded contingency tables (413–422); V. H. Vu, Spectral norm of random matrices (423–430); Terence Tao and Van Vu, On random $\pm 1$ matrices: singularity and determinant (431–440); Abraham D. Flaxman, Alan M. Frieze and Juan C. Vera, On the average case performance of some greedy approximation algorithms for the uncapacitated facility location problem (441–449).

Micah Adler, Jeff Edmonds and Jiří Matoušek, Towards asymptotic optimality in probabilistic packet marking (450–459); Yaoyun Shi, Tensor norms and the classical communication complexity of nonlocal quantum measurement (extended abstract) (460–467); Sean Hallgren, Fast quantum algorithms for computing the unit group and class group of a number field (468–474); Arthur Schmidt and Ulrich Vollmer, Polynomial time quantum algorithm for the computation of the unit group of a number field (extended abstract) (475–480); Michael Ben-Or and Avinatan Hassidim, Fast quantum Byzantine agreement (extended abstract) (481–485); Noga Alon, Konstantin Makarychev, Yury Makarychev and Assaf Naor, Quadratic forms on graphs (extended abstract) (486–493); Michael Elkin, Yuval Emek, Daniel A. Spielman and Shang-Hua Teng, Lower-stretch spanning trees (494–503); Daniel Gonçalves, Edge partition of planar graphs into two outerplanar graphs (504–512); Luis von Ahn, Nicholas Hopper and John Langford, Covert two-party computation (513–522); Hoeteck Wee, On obfuscating point functions (523–532).

Rafael Pass and Alon Rosen, New and improved constructions of non-malleable cryptographic protocols (533–542); Matt Lepinksi, Silvio Micali and Abhi Shelat, Collusion-free protocols (543–552); Sanjeev Arora, James R. Lee and Assaf Naor, Euclidean distortion and the sparsest cut (extended abstract) (553–562); Uriel Feige, Mohammad Taghi Hajiaghayi and James R. Lee, Improved approximation algorithms for minimum-weight vertex separators (extended abstract) (563–572) ; Amit Agarwal, Moses Charikar, Konstantin Makarychev and Yury Makarychev, $O(\sqrt{\log n})$ approximation algorithms for Min UnCut, Min 2CNF deletion, and directed cut problems (573–581); Joseph Naor and Roy Schwartz, Balanced metric labeling (extended abstract) (582–591) ; Zeev Dvir and Amir Shpilka, Locally decodable codes with 2 queries and polynomial identity testing for depth 3 circuits (592–601); Venkatesan Guruswami and Atri Rudra, Limits to list decoding Reed-Solomon codes (602–609); Shahar Dobzinski, Noam Nisan and Michael Schapira, Approximation algorithms for combinatorial auctions with complement-free bidders (610–618); Gagan Aggarwal, Amos Fiat, Andrew V. Goldberg, Jason D. Hartline, Nicole Immorlica and Madhu Sudan, Derandomization of auctions (619–625).

Vladimir Trifonov, An $O(\log n \log\log n)$ space algorithm for undirected st-connectivity (extended abstract) (626–633); Scott Aaronson, The complexity of agreement (634–643); Yael Tauman Kalai, Yehuda Lindell and Manoj Prabhakaran, Concurrent general composition of secure protocols in the timing model (644–653); Yevgeniy Dodis and

Adam Smith, Correcting errors without leaking partial information (654–663); Thomas Holenstein, Key agreement from weak bit agreement (664–673); Ferdinando Cicalese and Eduardo Sany Laber, A new strategy for querying priced information (674–683); Nir Ailon, Moses Charikar and Alantha Newman, Aggregating inconsistent information: ranking and clustering (684–693); Dimitris Achlioptas, Aaron Clauset, David Kempe and Cristopher Moore, On the bias of traceroute sampling or, power-law degree distributions in regular graphs (694–703); Christian Scheideler, How to spread adversarial nodes? Rotate! (704–713); Eli Gafni, Rachid Guerraoui and Bastian Pochon, From a static impossibility to an adaptive lower bound: the complexity of early deciding set agreement (714–722).
Prasad Jayanti, An optimal multi-writer snapshot algorithm (extended abstract) (723–732); Bogdan S. Chlebus and Dariusz R. Kowalski, Cooperative asynchronous update of shared memory (733–739); Johan Håstad, Every 2-CSP allows nontrivial approximation (740–746); W. Fernandez de la Vega, Ravi Kannan, Marek Karpinski and Santosh Vempala, Tensor decomposition and approximation schemes for constraint satisfaction problems (747–754); Klaus Jansen and Rob van Stee, On strip packing with rotations (755–761).
The articles of this volume will not be reviewed individually. The preceding conference has been reviewed (see Zbl 1074.68504).

*Classification* :

∗68-06 Proceedings of conferences (computer science)
00B25 Proceedings of conferences of miscellaneous specific interest
68R10 Graph theory in connection with computer science
68Q05 Models of computation
68W05 Nonnumerical algorithms

---

**Zbl pre05771425**

**Elkin, Michael; Emek, Yuval; Spielman, Daniel A.; Teng, Shang-Hua**
**Lower-stretch spanning trees.** (English)
STOC'05: Proceedings of the 37th annual ACM symposium on theory of computing, Baltimore, MD, USA, May 22–24, 2005. New York, NY: Association for Computing Machinery (ACM). 494-503 (2005). ISBN 1-58113-960-8
http://dx.doi.org/10.1145/1060590.1060665

Summary: We show that every weighted connected graph $G$ with $n$ vertices and $m$ edges contains as a subgraph a spanning tree into which the edges of $G$ can be embedded with average stretch $O(\log^2 n \log\log n)$. Moreover, we show that this tree can be constructed in time $O(m \log^2 n)$ in general, and in time $O(m \log n)$ if the input graph is unweighted. The main ingredient in our construction is a novel graph decomposition technique. Our new algorithm can be immediately used to improve the running time of the recent solver for symmetric diagonally dominant linear systems of Spielman and Teng from

$$m 2^{(O(\sqrt{\log n \log\log n}))} \text{ to } m \log^{O(1)} n,$$

and to $O(n \log^2 n \log\log n)$ when the system is planar. Our result can also be used to

improve several earlier approximation algorithms that use low-stretch spanning trees.

*Classification* :

∗05C05 Trees
05C85 Graphic algorithms
68Q25 Analysis of algorithms and problem complexity

---

**Zbl 1096.68778**

**Spielman, Daniel A.; Teng, Shang-hua; Üngör, Alper**
**Parallel Delaunay refinement with off-centers.** (English)
Danelutto, Marco (ed.) et al., Euro-Par 2004, parallel processing. 10th international Euro-Par conference, Pisa, Italy, August 31 – September 3, 2004. Proceedings. Berlin: Springer. Lecture Notes in Computer Science 3149, 812-819 (2004). ISBN 3-540-22924-8/pbk
http://dx.doi.org/10.1007/b99409

Summary: Off-centers were recently introduced as an alternative type of Steiner points to circum-centers for computing size-optimal quality guaranteed Delaunay triangulations. In this paper, we study the depth of the off-center insertion hierarchy. We prove that Delaunay refinement with off-centers takes only $O(\log(L/h))$ parallel iterations, where $L$ is the diameter of the domain, and $h$ is the smallest edge in the initial triangulation. This is an improvement over the previously best known algorithm that runs in $O(\log^2(L/h))$ iterations.

*Keywords* : Delaunay refinement; parallel algorithms; triangulations
*Classification* :

∗68W10 Parallel algorithms
68U05 Computational geometry, etc.

---

**Zbl 1074.68504**

**Proceedings of the 36th annual ACM symposium on theory of computing (STOC 2004), Chicago, IL, USA, June 13 - 15, 2004.** (English)
New York, NY: ACM Press. xvii, 643 p. $ 92.00 (2004). ISBN 1-58113-852-0
http://portal.acm.org/toc.cfm?id=1007352

Contents: Eli Ben-Sasson, Oded Goldreich, Prahladh Harsha, Madhu Sudan and Salil Vadhan, Robust PCPs of proximity, shorter PCPs and applications to coding 1–10; Jonas Holmerin and Subhash Khot, A new PCP outer verifier with applications to homogeneous linear equations and max-bisection 11–20; Julia Chuzhoy, Sudipto Guha, Eran Halperi [Eran Halperin], Sanjeev Khanna, Guy Kortsarz and Joseph Nao [Joseph Naor], Asymmetric $k$-center is $\log^* n$-hard to approximate 21–27; Julia Chuzhoy and Joseph Naor, New hardness results for congestion minimization and machine scheduling 28–34; Susanne Albers and Markus Schmidt, On the performance of greedy algorithms

in packet buffering 35–44; Baruch Awerbuch and Robert D. Kleinberg, Adaptive routing with end-to-end feedback: distributed learning and geometric approaches 45–53; Gurmeet Singh Manku, Moni Naor and Udi Wieder, Know thy neighbor's neighbor: the power of lookahead in randomized P2P networks 54–63; Yossi Azar and Yossi Richter, The zero-one principle for switching networks 64–71; Noga Alon and Assaf Naor, Approximating the cut-norm via Grothendieck's inequality 72–80; Daniel A. Spielman and Shang-Hua Teng, Nearly-linear time algorithms for graph partitioning, graph sparsification, and solving linear systems 81–90.

Richard Cole, Lee-Ad Gottlieb and Moshe Lewenstein, Dictionary matching and indexing with errors and don't cares 91–100; Irene Finocchi and Giuseppe F. Italiano, Sorting and searching in the presence of memory faults (without redundancy) 101–110; Andris Ambainis, Quantum algorithms a decade after Shor 111; Andrew Chi-Chih Yao, Graph entropy and quantum sorting problems 112–117; Scott Aaronson, Multilinear formulas and skepticism of quantum computing 118–127; Ziv Bar-Yossef, T. S. Jayram and Iordanis Kerenidis, Exponential separation of quantum and classical one-way communication complexity 128–137; G. Kortsarz and Z. Nutov, Approximation algorithm for $k$-node connected subgraphs via critical graphs 138–145; D. Bienstock and G. Iyengar, Solving fractional packing problems in $O^*(1/\epsilon)$ iterations 146–155; Chandra Chekuri, Sanjeev Khanna and F. Bruce Shepherd, The all-or-nothing multicommodity flow problem 156–165; Nikhil Bansal, Avrim Blum, Shuchi Chawla and Adam Meyerson, Approximation algorithms for deadline-TSP and vehicle routing with time-windows 166–174.

Artur Czumaj and Christian Sohler, Estimating the weight of metric minimum spanning trees in sublinear-time 175–183; Liam Roditty and Uri Zwick, A fully dynamic reachability algorithm for directed graphs with an almost linear update time 184–191; Alexander Healy, Salil Vadhan and Emanuele Viola, Using nondeterminism to amplify hardness 192–201; Rajeev Alur and P. Madhusudan, Visibly pushdown languages 202–211; Jianer Chen, Xiuzhen Huang, Iyad A. Kanj and Ge Xia, Linear FPT reductions and computational lower bounds 212–221; Sanjeev Arora, Satish Rao and Umesh Vazirani, Expander flows, geometric embeddings and graph partitioning 222–231; Rafael Pass, Bounded-concurrent secure multi-party computation with a dishonest majority 232–241; Manoj Prabhakaran and Amit Sahai, New notions of security: achieving universal composability without trusted setup 242–251; Danny Harnik, Moni Naor, Omer Reingold and Alon Rosen, Completeness in two-party secure computation: a computational view 252–261; Yuval Ishai, Eyal Kushilevitz, Rafail Ostrovsky and Amit Sahai, Batch codes and their applications 262–271.

Claire Kenyon, Yuval Rabani and Alistair Sinclair, Low distortion maps between point sets 272–280; Kunal Talwar, Bypassing the embedding: algorithms for low dimensional metrics 281–290; Sariel Har-Peled and Soham Mazumdar, On coresets for $k$-means and $k$-median clustering 291–300M Jean-Daniel Boissonnat, David Cohen-Steiner and Gert Vegter, Isotopic implicit surface meshing 301–309; László Lovász and Santosh Vempala, Hit-and-run from a corner 310–314; John Dunagan and Santosh Vempala, A simple polynomial-time rescaling algorithm for solving linear programs 315–320; Bogdan S. Chlebus, Dariusz R. Kowalski and Alexander A. Shvartsman, Collective asynchronous reading with polylogarithmic worst-case overhead 321–330; Michael Elkin, Unconditional lower bounds on the time-approximation tradeoffs for the distributed minimum spanning tree problem 331–340; Éva Tardos, Network games 341–342; Rene Beier and

Berthold Vöcking, Typical properties of winners and losers in discrete optimization 343–352.

Retsef Levi, Robin Roundy and David B. Shmoys, Primal-dual algorithms for deterministic inventory problems 353–362; Chandra Chekuri, Ashish Goel, Sanjeev Khanna and Amit Kumar, Multi-processor scheduling to minimize flow time with $\epsilon$ resource augmentation 363–372; Piotr Indyk, Algorithms for dynamic geometric problems over data streams 373–380; Tugkan Batu, Ravi Kumar [S. Ravi Kumar] and Ronitt Rubinfeld, Sublinear algorithms for testing monotone and unimodal distributions 381–390; Eldar Fischer, The difficulty of testing for isomorphism against a graph that is given in advance 391–397; José R. Correa and Michel X. Goemans, An approximate König's theorem for edge-coloring weighted bipartite graphs 398–406; Harold N. Gabow, Finding paths and cycles of superpolylogarithmic length 407–416; Anupam Gupta, Martin Pál, R. Ravi and Amitabh Sinha, Boosted sampling: approximation algorithms for stochastic optimization 417–426; Amir Shpilka and Avi Wigderson, Derandomizing homomorphism testing in general groups 427–435; Venkatesan Guruswami, Better extractors for better codes? 436–444; Eyal Rozenman, Aner Shalev and Avi Wigderson, A new family of Cayley expanders 445–454.

Jonathan A. Kelner, Spectral partitioning, eigenvalue bounds, and circle packings for graphs of bounded genus 455–464; Scott Aaronson, Lower bounds for local search by quantum arguments 465–474; Peter Burgisser and Felipe Cucker, Counting complexity classes for numeric computations. II. Algebraic and semialgebraic sets 475–485; Miklós Ajtai, A conjecture about polynomial time computable lattice-lattice functions 486–493; Miklos Santha and Mario Szegedy, Quantum and classical query complexities of local search are polynomially related 494–501; Ben W. Reichardt, The quantum adiabatic optimization algorithm and local minima 502–510; Rahul Garg and Sanjiv Kapoor, Auction algorithms for market equilibrium 511–518; Nikhil R. Devanur, The spending constraint model for market equilibrium: algorithmic, existence and uniqueness results 519–528; Jiangzhuo Chen, Robert D. Kleinberg, László Lovász, Rajmohan Rajaraman, Ravi Sundaram and Adrian Vetta, (Almost) tight bounds and existence theorems for confluent flows 529–538; Kenji Obata, Approximate max-integral-flow/min-multicut theorems 539–545; Mihai Pătraşcu and Erik D. Demaine, Lower bounds for dynamic connectivity 546–553.

Nir Ailon and Bernard Chazelle, Lower bounds for linear degeneracy testing 554–560; David Kempe and Frank McSherry, A decentralized algorithm for spectral analysis 561–568M Jon Kleinberg and Mark Sandler, Using mixture models for collaborative filtering 569–578; Avi Wigderson, Depth through breadth, or why should we attend talks in other areas? 579; Ashish Goel, Sanatan Rai and Bhaskar Krishnamachari, Sharp thresholds for monotone properties in random geometric graphs 580–586; Dimitris Achlioptas and Assaf Naor, The two possible values of the chromatic number of a random graph 587–593; Uriel Feige, On sums of independent random variables with unbounded variance, and estimating the average degree in a graph 594–603; Alex Fabrikant, Christos Papadimitriou and Kunal Talwar, The complexity of pure Nash equilibria 604–612; Martin Gairing, Thomas Lücking, Marios Mavronicolas and Burkhard Monien, Computing Nash equilibria for scheduling on restricted parallel links 613–622; Joseph Halpern and Vanessa Teague, Rational secret sharing and multiparty computation: extended abstract 623–632; Ran Raz, Multi-linear formulas for permanent and determinant are of

super-polynomial size 633–641.
Some articles of this volume will be reviewed individually. The preceding conference has been reviewed (see Zbl 1074.68503).

*Classification* :
*68-06 Proceedings of conferences (computer science)
00B25 Proceedings of conferences of miscellaneous specific interest
68Qxx Theory of computing

---

**Zbl pre05772157**

**Spielman, Daniel A.; Teng, Shang-Hua**
**Smoothed analysis of algorithms: why the simplex algorithm usually takes polynomial time.** (English)
J. ACM 51, No. 3, 385-463, electronic only (2004). ISSN 0004-5411
http://dx.doi.org/10.1145/990308.990310
http://portal.acm.org/browse_dl.cfm?linked=1part=journalidx=J401coll=ACMdl=ACMCFID=4

Summary: We introduce the smoothed analysis of algorithms, which continuously interpolates between the worst-case and average-case analyses of algorithms. In smoothed analysis, we measure the maximum over inputs of the expected performance of an algorithm under small random perturbations of that input. We measure this performance in terms of both the input size and the magnitude of the perturbations. We show that the simplex algorithm has smoothed complexity polynomial in the input size and the standard deviation of Gaussian perturbations.

*Classification* :
*90C05 Linear programming
90C60 Abstract computational complexity for math. programming problems
68W40 Analysis of algorithms

---

**Zbl pre05770686**

**Spielman, Daniel A.; Teng, Shang-Hua**
**Nearly-linear time algorithms for graph partitioning, graph sparsification, and solving linear systems.** (English)
Proceedings of the 36th annual ACM symposium on theory of computing (STOC 2004), Chicago, IL, USA, June 13 - 15, 2004. New York, NY: ACM Press. 81-90, electronic only (2004). ISBN 1-58113-852-0
http://dx.doi.org/10.1145/1007352.1007372

From the text: "We present a linear-system solver that, given an $n \times n$ symmetric diagonally-dominant matrix $A$ with $m$ non-zero entries and an $n$-vector $b$, produces a vector $\tilde{x}$ satisfying $A\tilde{x} - b < \epsilon$ and $\tilde{x} - x < \epsilon$, where $x$ is the solution to $Ax = b$, in time linear in $m$ and $\log(\kappa f(A)/\epsilon)$, where $\kappa f(A)$ is the condition number of $A$. Our

algorithm applies the preconditioned Chebyshev iteration with preconditioners designed using nearly-linear time algorithms for graph sparsification and graph partitioning.

*Classification* :

∗65F30 Other matrix algorithms
15A06 Linear equations (linear algebra)
05C85 Graphic algorithms
05C70 Factorization, etc.
68R10 Graph theory in connection with computer science

---

**Zbl 1074.68503**

**Proceedings of the thirty-fifth annual ACM symposium on theory of computing (STOC 2003), San Diego, CA, USA,.** (English)
New York, NY: ACM Press. xii, 728 p. $ 104.00 (2003). ISBN 1-58113-674-9
http://portal.acm.org/toc.cfm?id=780542

Contents: Joel Friedman, A proof of Alon's second eigenvalue conjecture 720–724; Toshiya Itoh, Yoshinori Takei and Jun Tarui, On the sample size of $k$-restricted min-wise independent permutations and other distributions 710–719; Noga Alon and Asaf Shapira, Testing subgraphs in directed graphs 700–709; Martin Dyer, Approximate counting by dynamic programming 693–699; Yehuda Lindell, Bounded-concurrent secure two-party computation without setup assumptions 683–692; T. S. Jayram, Ravi Kumar and D. Sivakumar, Two applications of information complexity 673–682; T. S. Jayram, Subhash Khot, Ravi Kumar and Yuval Rabani, Cell-probe lower bounds for the partial match problem 667–672; Anna Gal and Adi Rosen, Lower bounds on the amount of randomness in private computation 659–666; Mikkel Thorup, Space efficient dynamic stabbing with fast queries 649–658; Haim Kaplan, Eyal Molad and Robert E. Tarjan, Dynamic rectangular intersection with priorities 639–648.
Martin Dietzfelbinger and Philipp Woelfel, Almost random graphs with simple hash functions 629–638; Anna Ostlin and Rasmus Pagh, Uniform hashing in constant time and linear space 622–628; Eli Ben-Sasson, Madhu Sudan, Salil Vadhan and Avi Wigderson, Randomness-efficient low degree tests and short PCPs via epsilon-biased sets 612–621; Chi-Jen Lu, Omer Reingold, Salil Vadhan and Avi Wigderson, Extractors: optimal up to constant factors 602–611; Irit Dinur, Venkatesan Guruswami, Subhash Khot and Oded Regev, A new multilayered PCP and the hardness of hypergraph vertex cover 595–601; Eran Halperin and Robert Krauthgamer, Polylogarithmic inapproximability 585–594; Micah Adler, Eran Halperin, Richard M. Karp and Vijay V. Vazirani, A stochastic process on the hypercube with applications to peer-to-peer networks 575–584; Robert Kleinberg and Tom Leighton, Consistent load balancing via spread minimization 565–574; Adam L. Buchsbaum, Howard Karloff, Claire Kenyon, Nick Reingold and Mikkel Thorup, OPT versus LOAD in dynamic storage allocation 556–564.
Boris Aronov, Vladlen Koltun and Micha Sharir, Cutting triangular cycles of lines in space 547–555; Boris Aronov, János Pach, Micha Sharir and Gábor Tardos, Distinct distances in three and higher dimensions 541–546; Bernard Chazelle, Ding Liu and Avner Magen, Sublinear geometric algorithms 531–540; Richard Cole, Yevgeniy Dodis and

Tim Roughgarden, Pricing network edges for heterogeneous selfish users 521–530; Elliot Anshelevich, Anirban Dasgupta, Eva Tardos and Tom Wexler, Near-optimal network design with selfish agents 511–520; Baruch Awerbuch, Yossi Azar and Adam Meyerson, Reducing truth-telling online mechanisms to online optimization 503–510; Tamal K. Dey, Joachim Giesen and Matthias John, Alpha-shapes and flow shapes are homotopy equivalent 493–502; Jie Gao and Li Zhang, Well-separated pair decomposition for the unit-disk graph metric and its applications 483–492; Moshe Dror, Alon Efrat, Anna Lubiw and Joseph S. B. Mitchell, Touring a sequence of polygons 473–482; Yair Bartal, Nathan Linial, Manor Mendel and Assaf Naor, On metric Ramsey-type phenomena 463–472.

Yuri Rabinovich, On average distortion of embedding metrics into the line and into $L_1$ 456–462; Jittat Fakcharoenphol, Satish Rao and Kunal Talwar, A tight bound on approximating arbitrary metrics by tree metrics 448–455; Robert Krauthgamer and James R. Lee, The intrinsic dimensionality of graphs 438–447; Ivan Damgard and Jens Groth, Non-interactive and reusable non-malleable commitment schemes 426–437; Rosario Gennaro, Yael Gertner and Jonathan Katz, Lower bounds on the efficiency of encryption and digital signature schemes 417–425; Oded Regev, New lattice based cryptographic constructions 407–416M; Miklos Ajtai, The worst-case behavior of Schnorr's algorithm approximating the shortest nonzero vector in a lattice 396–4063; Jochen Könemann and R. Ravi, Primal-dual meets local search: approximating MST's with nonuniform degree bounds 389–395; Yossi Azar, Edith Cohen, Amos Fiat, Haim Kaplan and Harald Racke, Optimal oblivious routing in polynomial time 383–388; Jiangzhuo Chen, Rajmohan Rajaraman and Ravi Sundaram, Meet and merge: approximation algorithms for confluent flows 373–382.

Anupam Gupta, Amit Kumar and Tim Roughgarden, Simpler and better approximation algorithms for network design 365–372; Valentine Kabanets and Russell Impagliazzo, Derandomizing polynomial identity tests means proving circuit lower bounds 355–364; Eli Ben-Sasson, Prahladh Harsha and Sofya Raskhodnikova, Some 3CNF properties are hard to test 345–354; Ziv Bar-Yossef, Sampling lower bounds via information theory 335–344; Ryan O'Donnell and Rocco A. Servedio, New degree bounds for polynomial threshold functions 325–334; Tugkan Batu, Funda Ergün, Joe Kilian, Avner Magen, Sofya Raskhodnikova, Ronitt Rubinfeld and Rahul Sami, A sublinear algorithm for weakly approximating edit distance 316–324; Gerth Stølting Brodal and Rolf Fagerberg, On the limits of cache-obliviousness 307–315; Anna Gilbert and Howard Karloff, On the fractal behavior of TCP 297–306; Sergey Bobkov and Prasad Tetali, Modified log-Sobolev inequalities, mixing and hypercontractivity 287–296.

Ben Morris and Yuval Peres, Evolving sets and mixing 279–286; Thomas P. Hayes, Randomly coloring graphs of girth at least five 269–278; Panagiota Fatourou, Faith Fich and Eric Ruppert, A tight lower bound for space-optimal implementations of multi-writer snapshots 259–268; Chryssis Georgiou, Alexander Russell and Alex A. Shvartsman, Work-competitive scheduling for cooperative computing with dynamic groups 251–258; Nikhil Bansal and Kirk Pruhs, Server scheduling in the $L_p$ norm: a rising tide lifts all boat 242–250; Rene Beier and Berthold Vöcking, Random knapsack in expected polynomial time 232–241; Dimitris Achlioptas and Yuval Peres, The threshold for random $k$-SAT is $2^k(\ln 2 - O(k))$ 223–231; Jeong Han Kim and Van H. Vu, Generating random regular graphs 213–222; Elchanan Mossel, Ryan O'Donnell and Rocco P. Servedio,

Learning juntas 206–212; Adam Kalai and Rocco A. Servedio, Boosting in the presence of noise 195–205.
Martin Sauerhoff and Philipp Woelfel, Time-space tradeoff lower bounds for integer multiplication and graphs of arithmetic functions 186–195; Robert Rettinger and Klaus Weihrauch, The computational complexity of some Julia sets 177–185; Richard Cole and Ramesh Hariharan, A fast algorithm for computing Steiner edge connectivity 167–176; Camil Demetrescu and Giuseppe F. Italiano, A new approach to dynamic all pairs shortest paths 159–166; Mikkel Thorup, Integer priority queues with decrease key in constant time and the single source shortest paths problem 149–158; Lukasz Kowalik and Maciej Kurowski, Short path queries in planar graphs in constant time 143–148; Don Coppersmith and Madhu Sudan, Reconstructing curves in three (and higher) dimensional space from noisy data 136–142; Venkatesan Guruswami and Piotr Indyk, Linear time encodable and list decodable codes 126–135; Gábor Tardos, Optimal probabilistic fingerprint codes 116–125; Iordanis Kerenidis and Ronald de Wolf, Exponential lower bound for 2-query locally decodable codes via a quantum argument 106–115M.
Eyal Amir, Robert Krauthgamer and Satish Rao, Constant factor approximation of vertex-cuts in planar graphs 90–99; Noga Alon, Baruch Awerbuch and Yossi Azar, The online set cover problem 100–105; Yossi Azar and Yossi Richter, Management of multi-queue switches in QoS networks 82–89; Andrew Chi-Chih Yao, On the power of quantum fingerprinting 77–81; Hartmut Klauck, Quantum time-space tradeoffs for sorting 69–76; Andrew M. Childs, Richard Cleve, Enrico Deotto, Edward Farhi, Sam Gutmann and Daniel A. Spielman, Exponential algorithmic speedup by a quantum walk 59–68; W. Fernandez de la Vega, Marek Karpinski, Claire Kenyon and Yuval Rabani, Approximation schemes for clustering problems 50–58; C. Greg Plaxton, Approximation algorithms for hierarchical location problems 40–49; Moses Charikar, Liadan O'Callaghan and Rina Panigrahy, Better streaming algorithms for clustering problems 30–39; Dorit Aharonov and Amnon Ta-Shma, Adiabatic quantum state generation and statistical zero knowledge 20–29; Katalin Friedl, Gábor Ivanyos, Frédéric Magniez, Miklos Santha and Pranab Sen, Hidden translation and orbit coset in quantum computing 1–9; Leonid Gurvits, Classical deterministic complexity of Edmond's problem and quantum entanglement 10–19.
Some articles of this volume will be reviewed individually. The preceding conference has been reviewed (see Zbl 1074.68502).

*Classification* :

∗68-06 Proceedings of conferences (computer science)
00B25 Proceedings of conferences of miscellaneous specific interest
68Qxx Theory of computing

---

**Zbl 1035.90042**

**Spielman, Daniel A.; Teng, Shang-Hua**

**Smoothed analysis of termination of linear programming algorithms.** (English)

Math. Program. 97, No. 1-2 (B), 375-404 (2003). ISSN 0025-5610; ISSN 1436-4646
http://dx.doi.org/10.1007/s10107-003-0448-9
http://link.springer.de/link/service/journals/10107/

Summary: We perform a smoothed analysis of a termination phase for linear programming algorithms. By combining this analysis with the smoothed analysis of Renegar's condition number by *J. Dunagan, D. A. Spielman* and *S.-H. Teng* [Smoothed analysis of termination of linear programming algorithms. (`http://arxiv.org/abs/cs.DS/0302011`] we show that the smoothed complexity of interior-point algorithms for linear programming is $O(m^3 \log(m/\sigma))$. In contrast, the best known bound on the worst-case complexity of linear programming is $O(m^3 L)$, where $L$ could be as large as $m$. We include an introduction to smoothed analysis and a tutorial on proof techniques that have been useful in smoothed analyses.

*Classification* :

∗90C05 Linear programming
90C51 Interior-point methods
68Q25 Analysis of algorithms and problem complexity
68W40 Analysis of algorithms

---

**Zbl pre05771042**

**Childs, Andrew M.; Cleve, Richard; Deotto, Enrico; Farhi, Edward; Gutmann, Sam; Spielman, Daniel A.**
**Exponential algorithmic speedup by a quantum walk.** (English)
Proceedings of the thirty-fifth annual ACM symposium on theory of computing (STOC 2003), San Diego, CA, USA,. New York, NY: ACM Press. 59-68, electronic only (2003). ISBN 1-58113-674-9
http://dx.doi.org/10.1145/780542.780552

Summary: We construct a black box graph traversal problem that can be solved exponentially faster on a quantum computer than on a classical computer. The quantum algorithm is based on a continuous time quantum walk, and thus employs a different technique from previous quantum algorithms based on quantum Fourier transforms. We show how to implement the quantum walk efficiently in our black box setting. We then show how this quantum walk solves our problem by rapidly traversing a graph. Finally, we prove that no classical algorithm can solve the problem in subexponential time.

*Classification* :

∗81P68 Quantum computation and quantum cryptography
68Q05 Models of computation

---

**Zbl pre05695505**

**Spielman, Daniel A.; Teng, Shang-Hua**
**Smoothed analysis. Motivation and discrete models.** (English)
Dehne, Frank (ed.) et al., Algorithms and data structures. 8th international workshop, WADS 2003, Ottawa, Ontario, Canada, July 30 – August 1, 2003. Proceedings. Berlin: Springer. Lect. Notes Comput. Sci. 2748, 256-270 (2003). ISBN 3-540-40545-3/pbk

http://dx.doi.org/10.1007/b11837

Summary: In smoothed analysis, one measures the complexity of algorithms assuming that their inputs are subject to small amounts of random noise. In an earlier work (Spielman and Teng, 2001), we introduced this analysis to explain the good practical behavior of the simplex algorithm. In this paper, we provide further motivation for the smoothed analysis of algorithms, and develop models of noise suitable for analyzing the behavior of discrete algorithms. We then consider the smoothed complexities of testing some simple graph properties in these models.

*Classification* :
∗68P10 Searching and sorting
68Wxx Algorithms

---

**Zbl 1056.65148**

**Spielman, Daniel A.; Teng, Shang-Hua**
**Smoothed analysis of algorithms.** (English)
Li, Ta Tsien (ed.) et al., Proceedings of the international congress of mathematicians, ICM 2002, Beijing, China, August 20–28, 2002. Vol. I: Plenary lectures and ceremonies. Beijing: Higher Education Press; Singapore: World Scientific/distributor. 597-606 (2002). ISBN 7-04-008690-5/3 vol. set

The authors survey the so-called smoothed analysis, which is their modification of Smale's complexity theory of numerical algorithms.

*Ping-Qi Pan (Nanjing)*
*Keywords* : smoothed (complexity) analysis; condition number; simplex method; interior point method; perceptron method; numerical algorithms
*Classification* :
∗65Y20 Complexity and performance of numerical algorithms
68Q25 Analysis of algorithms and problem complexity
90C05 Linear programming
90C51 Interior-point methods
65K05 Mathematical programming (numerical methods)
68Q17 Computational difficulty of problems

---

**Zbl 1019.94032**

**Luby, Michael G.; Mitzenmacher, Michael; Shokrollahi, M.Amin; Spielman, Daniel A.**
**Efficient erasure correcting codes.** (English)
IEEE Trans. Inf. Theory 47, No.2, 569-584 (2001). ISSN 0018-9448
http://dx.doi.org/10.1109/18.910575
http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?puNumber=18

Summary: We introduce a simple erasure recovery algorithm for codes derived from cascades of sparse bipartite graphs and analyze the algorithm by analyzing a corresponding discrete-time random process. As a result, we obtain a simple criterion involving the fractions of nodes of different degrees on both sides of the graph which is necessary and sufficient for the decoding process to finish successfully with high probability. By carefully designing these graphs we can construct for any given rate $R$ and any given real number $\varepsilon$ a family of linear codes of rate $R$ which can be encoded in time proportional to $\ln(1/\varepsilon)$ times their block length $n$. Furthermore, a codeword can be recovered with high probability from a portion of its entries of length $(1+\varepsilon)Rn$ or more. The recovery algorithm also runs in time proportional to $n\ln(1/\varepsilon)$. Our algorithms have been implemented and work well in practice; various implementation issues are discussed.

*Keywords* : erasure channel; large deviation analysis; low-density parity-check codes; sparse bipartite graphs
*Classification* :
∗94B60 Other types of codes
05C90 Appl. of graph theory
94B35 Decoding
94A40 Channel models

---

**Zbl 0999.94042**

**Luby, Michael G.; Mitzenmacher, Michael; Shokrollahi, M.Amin; Spielman, Daniel A.**

**Improved low-density parity-check codes using irregular graphs.** (English)
IEEE Trans. Inf. Theory 47, No.2, 585-598 (2001). ISSN 0018-9448
http://dx.doi.org/10.1109/18.910576
http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?puNumber=18

Summary: We construct new families of error-correcting codes based on Gallager's low-density parity-check codes. We improve on Gallager's results by introducing irregular parity-check matrices and a new rigorous analysis of hard-decision decoding of these codes. We also provide efficient methods for finding good irregular structures for such decoding algorithms. Our rigorous analysis based on martingales, our methodology for constructing good irregular codes, and the demonstration that irregular structure improves performance constitute key points of our contribution.
We also consider irregular codes under belief propagation. We report the results of experiments testing the efficacy of irregular codes on both binary symmetric and Gaussian channels. For example, using belief propagation, for rate 1/4 codes on 16000 bits over a binary symmetric channel, previous low-density parity-check codes can correct up to approximately 16% errors, while our codes correct over 17%. In some cases our results come very close to reported results for turbo codes, suggesting that variations of irregular low-density parity-check codes may be able to match or beat turbo code performance.

*Keywords* : Gallagher codes; concentration theorem; low-density parity-check codes; hard-decision decoding; irregular codes; belief propagation

*Classification* :

∗94B60 Other types of codes
94B35 Decoding
94B65 Bounds on codes

---

**Zbl 0972.68086**

**Kiwi, M.; Spielman, D.A.; Teng, S.-H.**

**Min-max-boundary domain decomposition.** (English)

Theor. Comput. Sci. 261, No.2, 253-266 (2001). ISSN 0304-3975
http://dx.doi.org/10.1016/S0304-3975(00)00143-2
http://www.sciencedirect.com/science/journal/03043975

Summary: Domain decomposition is one of the most effective and popular parallel computing techniques for solving large-scale numerical systems. In the special case when the amount of computation in a subdomain is proportional to the volume of the subdomain, domain decomposition amounts to minimizing the surface area of each subdomain while dividing the volume evenly. Motivated by this fact, we study the following min-max-boundary multi-way partitioning problem. Given a graph $G$ and an integer $k > 1$, we would like to divide $G$ into $k$ subgraphs $G_1, \ldots, G_k$ (by removing edges) such that (i) $|G_i| = \Theta(|G|/k)$ for all $i \in 1, \ldots, k$; and (ii) the maximum boundary size of any subgraph (the set of edges connecting it with other subgraphs) is minimized. We provide an algorithm that given $G$, a well-shaped mesh in $d$ dimensions, finds a partition of $G$ into $k$ subgraphs $G_1, \ldots, G_k$, such that for all $i$, $G_i$ has $\Theta(|G|/k)$ vertices and the number of edges connecting $G_i$ with the other subgraphs is $O((|G|/k)^{1-1/d})$. Our algorithm can find such a partition in $O(|G| \log k)$ time. Finally, we extend our results to vertex-weighted and vertex-based graph decomposition. Our results can be used to simultaneously balance the computational and memory loads on a distributed-memory parallel computer without incurring large communication overhead. c.

*Keywords* : surface-to-volume ratio; communication to computation ratio; domain decomposition; multi-way partitioning; parallel processing

*Classification* :

∗68Q10 Modes of computation

---

**Zbl 0986.68135**

**Kiwi, Marcos; Lund, Carsten; Spielman, Daniel; Russell, Alexander; Sundaram, Ravi**

**Alternation in interaction.** (English)

Comput. Complexity 9, No.3-4, 202-246 (2000). ISSN 1016-3328; ISSN 1420-8954
http://dx.doi.org/10.1007/PL00001607
http://link.springer.de/link/service/journals/00037/

Summary: The traditional studies of multi-prover interactive proof systems have con-

centrated on cooperating provers. These are systems in which a verifier interacts with a set of provers who collaborate in their attempt to convince the verifier that a word $\omega$ is in a prespecified language $L$. Results on probabilistically checkable proofs coupled with parallel repetition techniques characterize NP in terms of multi-prover proof systems: languages in NP can be verified through a one-round interaction with two cooperating provers using limited randomness and communication.
Less attention has been paid to the study of competition in this complexity-theoretic setting of interactive proof systems. We consider, for example, one-round proof systems where the first prover is trying to convince the verifier to accept and the second prover is trying to convince the verifier to reject. We build into these proof systems a (crucial) asymmetry between the provers, analogous to quantifier alternation. We show that such proof systems capture, with restrictions on communication and randomness, languages in NP. We generalize this model by defining alternating prover proof systems which we show characterize each level of the polynomial hierarchy. Alternating oracle proof systems are also examined.
The main contribution of this work is the first exact characterization of the polynomial hierarchy in terms of interactive (prover) proof systems.

*Keywords* : cooperating provers; interactive proof systems
*Classification* :
∗68T15 Theorem proving
68Q15 Complexity classes of computation
91A10 Noncooperative games

---

**Zbl 0986.94045**

**Spielman, Daniel A.**

**Constructing error-correcting codes from expander graphs.** (English)

Hejhal, Dennis A. (ed.) et al., Emerging applications of number theory. Based on the proceedings of the IMA summer program, Minneapolis, MN, USA, July 15-26, 1996. New York, NY: Springer. IMA Vol. Math. Appl. 109, 591-600 (1999). ISBN 0-387-98824-6/hbk

Author's summary: We survey a derivation of asymptotically good error-correcting codes from expander graphs. These codes, called expander codes, can be decoded in linear time. We explain how to modify this construction to produce asymptotically good codes that can be encoded as well as decoded in linear time.

*Patrick Fitzpatrick (Cork)*

*Keywords* : asymptotically good error correcting codes; expander graphs; decoding; expander codes
*Classification* :
∗94B60 Other types of codes
05C90 Appl. of graph theory
05C50 Graphs and matrices
94B35 Decoding

---

**Zbl 0962.68062**

**Luby, Michael G.; Mitzenmacher, Michael; Shokrollahi, M.Amin; Spielman, Daniel A.; Stemann, Volker**

**Practical loss-resilient codes.** (English)

STOC '97. Proceedings of the 29th annual ACM symposium on theory of computing, El Paso, TX, USA, May 4-6, 1997. New York, NY: ACM, Association for Computing Machinery, 150-159 (1999).

Summary: We present randomized constructions of linear-time encodable and decodable codes that can transmit over lossy channels at rates extremely close to capacity. The encoding and decoding algorithms for these codes have fast and simple software implementations. Partial implementations of our algorithms are faster by orders of magnitude than the best software implementations of any previous algorithm for this problem. We expect these codes will be extremely useful for applications such as real-time audio and video transmission over the Internet, where lossy channels are common and fast decoding is a requirement. Despite the simplicity of the algorithms, their design and analysis are mathematically intricate. The design requires the careful choice of a random irregular bipartite graph, where the structure of the irregular graph is extremely important. We model the progress of the decoding algorithm by a set of differential equations. The solution to these equations can then be expressed as polynomials in one variable with coefficients determined by the graph structure. Based on these polynomials, we design a graph structure that guarantees successful decoding with high probability.

*Keywords* : encoding algorithms; decoding algorithms
*Classification* :
∗68P30 Coding and information theory
68W05 Nonnumerical algorithms

---

**Zbl 1027.68604**

**Luby, Michael G.; Mitzenmacher, Michael; Shokrollahi, M.Amin; Spielman, Daniel A.**

**Analysis of low density codes and improved designs using irregular graphs.** (English)

STOC '98. Proceedings of the 30th annual ACM symposium on theory of computing, Dallas, TX, USA, May 23-26, 1998. New York, NY: ACM, Association for Computing Machinery. 249-258 (1998). ISBN 0-89791-962-9

In 1963 Gallager introduces a family of codes based on sparse bipartite graphs, which he calls low-density parity-check codes. He suggests a natural decoding algorithm for these codes, and proves a good bound on the fraction of errors that can be corrected. As the codes that Gallager builds are derived from regular graphs, we refer to them as regular codes.
Following the general approach introduced in *M. Luby*, *M. Mitzenmacher*, *M. A. Shokrollahi*, *D. A. Spielman* and *V. Stemann* [Practical Loss-Resilient Codes, Proc. 29th Symp. on Theory of Computing, 150-159 (1997)] for the design and analysis of erasure codes,

we consider error-correcting codes based on random irregular bipartite graphs, which we call irregular codes. We introduce tools based on linear programming for designing linear time irregular codes with better error-correcting capabilities than possible with regular codes. For example, the decoding algorithm for the rate 1/2 regular codes of Gallager can provably correct up to 5.17% errors asymptotically, whereas we have found irregular codes for which our decoding algorithm can provably correct up to 6.27% errors asymptotically. We include the results of simulations demonstrating the effectiveness of our codes on systems of reasonable size.

*Keywords* : decoding algorithm; regular codes
*Classification* :
*68P30 Coding and information theory
68R10 Graph theory in connection with computer science

---

**Zbl 0935.68026**

**Spielman, Daniel A.**
**Models of computation in coding theory.** (English)
Thirteenth annual IEEE conference on Computational complexity. Proceedings of the conference held in Buffalo, NY, USA, June 15-18, 1998. Los Alamitos, CA: IEEE Computer Society. 120-131 (1998). ISBN 0-8186-8395-3

Summary: We contrast some fundamental assumption of coding theory with those used in complexity theory. In particular, we explain the differences in algorithm used in the software and hardware implementations of Reed-Solomon codes. We also explain how, when studying error-correcting codes, one must consider energy and communication delay to be resources, in addition to the usual space and time.

*Keywords* : coding theory; complexity theory
*Classification* :
*68Q05 Models of computation

---

**Zbl 0909.68075**

**Kiwi, Marcos; Spielman, Daniel A.; Teng, Shang-Hua**
**Min-max-boundary domain decomposition.** (English)
Hsu, Wen-Lian (ed.) et al., Computing and combinatorics. 4th annual international conference, COCOON '98, Taipei, Taiwan, ROC, August 12–14, 1998. Proceedings. Berlin: Springer. Lect. Notes Comput. Sci. 1449, 137-146 (1998). ISBN 3-540-64824-0

Summary: Domain decomposition is one of the most effective and popular parallel computing techniques for solving large scale numerical systems. In the special case when the amount of computation in a subdomain is proportional to the volume of the subdomain, domain decomposition amounts to minimizing the surface area of each subdomain while dividing the volume evenly. Motivated by this fact, we study the following min-max boundary multi-way partitioning problem: Given a graph $G$ and an integer $k > 1$, we would like to divide $G$ into $k$ subgraphs $G_1, \ldots, G_k$ (by removing edges) such that (i) $|G_i| = \Theta(|G|/k)$ for all $i \in \{1, \ldots, k\}$; and (ii) the maximum

boundary size of any subgraph (the set of edges connecting it with other subgraphs) is minimized.
We provide an algorithm that given $G$, a well-shaped mesh in $d$ dimensions, finds a partition of $G$ into $k$ subgraphs $G_1, \ldots, G_k$, such that for all $i$, $G_i$ has $\Theta(|G|/k)$ vertices and the number of edges connecting $G_i$ with the othe subgraphs is $O((|G|/k)^{1-1/d})$. Our algorithm can find such a partition in $O(|G| \log k)$ time. Finally, we extend our results to vertex-weighted and vertex-based graph decomposition. Our results can be used to simultaneously balance the computational and memory requirement on a distributed-memory parallel computer without sacrificing the communication overhead.

*Keywords* : domain decomposition; large scale numerical systems
*Classification* :
∗68Q10 Modes of computation

---

**Zbl 0943.94544**

**Spielman, Daniel A.**

**Linear-time encodable and decodable error-correcting codes.** (English)
IEEE Trans. Inf. Theory 42, No.6, Pt. 1, 1723-1731 (1996). ISSN 0018-9448
http://dx.doi.org/10.1109/18.556668
http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?puNumber=18

Summary: The author presents a new class of asymptotically good, linear error-correcting codes. These codes can be both encoded and decoded in linear time. They can also be encoded by logarithmic-depth circuits of linear size and decoded by logarithmic-depth circuits of size $O(n \log n)$. He presents both randomized and explicit constructions of these codes.

*Keywords* : expander graph; superconcentrators; linear error-correcting codes
*Classification* :
∗94B05 General theory of linear codes
94B35 Decoding

---

**Zbl 0943.94543**

**Sipser, Michael**; **Spielman, Daniel A.**

**Expander codes.** (English)
IEEE Trans. Inf. Theory 42, No.6, Pt. 1, 1710-1722 (1996). ISSN 0018-9448
http://dx.doi.org/10.1109/18.556667
http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?puNumber=18

Summary: Using expander graphs, the authors construct a new family of asymptotically good, linear error-correcting codes. These codes have linear time sequential decoding algorithms and logarithmic time parallel decoding algorithms that use a linear number of processors. They present both randomized and explicit constructions of these codes. Experimental results demonstrate the good performance of the randomly chosen codes.

*Keywords* : expander graphs; linear error-correcting codes; linear time sequential decoding algorithms

*Classification* :

∗94B05 General theory of linear codes

94B35 Decoding

---

**Zbl 0942.00501**

**Feigenbaum, Joan (ed.); Forney, G.David jun. (ed.); Marcus, Brian H. (ed.); McEliece, Robert J. (ed.); Vardy, Alexander (ed.)**

**Special issue on codes and complexity.** (English)

IEEE Trans. Inf. Theory 42, No.6, Pt. 1, 1649-2064 (1996). ISSN 0018-9448

http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?puNumber=18

Contents: Hans-Andrea Loeliger and Thomas Mittelholzer, Convolutional codes over groups (1660-1686); Aaron B. Kiely, Samuel J. Dolinar, jun., Robert J. McEliece, Laura L. Ekroot and Wei Lin, Trellis decoding complexity of linear block codes (1687-1697); Lance C. Perez, Jan Seghers and Daniel J. Costello, jun., A distance spectrum interpretation of turbo codes (1698-1709); Michael Sipser and Daniel A. Spielman, Expander codes (1710-1722); Daniel A. Spielman, Linear-time encodable and decodable error-correcting codes (1723-1731); Noga Alon and Michael Luby, A linear time erasure-resilient code with nearly optimal recovery (1732-1736); Andres Albanese, Johannes Blomer, Jeff Edmonds, Michael Luby and Madhu Sudan, Priority encoding transmission (1737-1744); Leonard J. Schulman, Coding for interactive communication (1745-1756); Jacques Stern, A new paradigm for public key identification (1757-1768); Gilles Brassard, Claude Crepeau and Miklos Santha, Oblivious transfers and intersecting codes (1769-1780); Mihir Bellare, Don Coppersmith, Johan Hastad, Marcos Kiwi and Madhu Sudan, Linearity testing in characteristic two (1781-1795). Vahid Tarokh and Ian F. Blake, Trellis complexity versus the coding gain of lattices. I (1796-1807); Vahid Tarokh and Ian F. Blake, Trellis complexity versus the coding gain of lattices. II (1808-1816); Yuval Berger and Yair Be'ery, The twisted squaring construction, trellis complexity, and generalized weights of BCH and QR codes (1817-1827); Frank R. Kschischang, The trellis structure of maximal fixed-cost codes (1828-1838); Vijay Vazirani, Huzur Saran and B. Sundar Rajan, An efficient algorithm for constructing minimal trellises for codes over finite abelian groups (1839-1854); Robert J. McEliece and Wei Lin, The trellis complexity of convolutional codes (1855-1864); G. David Forney, Jr., Rolf Johannesson and Zhe-xian Wan, Minimal and canonical rational generator matrices for convolutional codes (1865-1880); Joachim Rosenthal, J. M. Schumacher and Eric V. York, On behaviors and convolutional codes (1881-1891); Fabio Fagnani and Sandro Zampieri, dynamical systems and convolutional codes over finite abelian groups (1892-1912); Jonathan J. Ashley, A linear bound for sliding-block decoder window size. II (1913-1924); Jonathan J. Ashley, Razmik Karabed and Paul H. Siegel, Complexity and sliding-block decodability (1925-1947). Jonathan J. Ashley, Brian H. Marcus and Ron M. Roth, On the decoding delay of encoders for input-constrained channels (1948-1956); Henk D. L. Hollmann, Bounded-delay-encodable, block-decodable codes

for constrained systems (1957-1970); Ilya Dumer, Suboptimal decoding of linear codes: partition technique (1971-1986); Ba-Zhong Shen, Kenneth K. Tzeng and Chun Wang, A bounded-distance decoding algorithm for binary linear block codes achieving the minimum effective error coefficient (1987-1991); G. David Forney, Jr. and Alexander Vardy, Generalized minimum-distance decoding of Euclidean-space codes and lattices (1992-2026); Alexander Vardy and Frank R. Kschischang, Proof of a conjecture of McEliece regarding the expansion index of the minimal trellis (2027-2034); Petra Schuurman, A table of state complexity bounds for binary linear codes (2034-2042); Gavin B. Horn and Frank R. Kschischang, On the intractability of permuting a block code to minimize trellis complexity (2042-2048); Vladimir Sidorenko, Garik Markarian and Bahram Honary, Minimal trellis design for linear codes based on the Shannon product (2048-2053); Gerard D. Cohen, Simon Litsyn and Gilles Zemor, On greedy algorithms in coding theory (2053-2057).
The articles of this volume will be reviewed individually.

*Keywords* : Special issue; Codes; Complexity
*Classification* :
∗00B25 Proceedings of conferences of miscellaneous specific interest
94-06 Proceedings of conferences (information and communication)
94Bxx Theory of error-correcting codes

---

**Zbl 0915.05104**

**Spielman, Daniel A.**

**Faster isomorphism testing of strongly regular graphs.** (English)
Proceedings of the 28th annual ACM symposium on the theory of computing (STOC). Philadelphia, PA, USA, May 22–24, 1996. New York, NY: ACM, 576-584 (1996).

Summary: We demonstrate that isomorphism of strongly regular graphs may be tested in time $n^{O(n^{1/3}\log n)}$. Our approach is to analyze the standard individualization and refinement algorithm in light of Neumaier's claw bound, which implies that low degree strongly regular graphs have a small second-largest eigenvalue, unless they are Steiner or Latin square graphs.

*Keywords* : isomorphism of strongly regular graphs; refinement algorithm; eigenvalue
*Classification* :
∗05C85 Graphic algorithms
05E30 Association schemes, etc.
68R10 Graph theory in connection with computer science
05C60 Isomorphism problems (graph theory)

---

**Zbl 1058.94525**

**Spielman, Daniel A.**

**Linear-time encodable and decodable error-correcting codes.** (English)
Proceedings of the 27th annual ACM symposium on the theory of computing (STOC). Las Vegas, NV, USA, May 29 - June 1, 1995. New York, NY: ACM. 388-397 (1995).

See the journal version in IEEE Trans. Inf. Theory 42, No. 6, Pt. 1, 1723–1731 (1996; Zbl 0943.94544).

*Classification* :

*94B05 General theory of linear codes

94B35 Decoding

---

**Zbl 0827.68040**

**Beigel, Richard**; **Reingold, Nick**; **Spielman, Daniel**

**PP is closed under intersection.** (English)

J. Comput. Syst. Sci. 50, No.2, 191-202 (1995). ISSN 0022-0000

http://dx.doi.org/10.1006/jcss.1995.1017

http://www.sciencedirect.com/science/journal/00220000

Summary: In this seminal paper on probabilistic Turing machines, Gill asked whether the class PP is closed under intersection and union. We give a positive answer to this question. We also show that PP is closed under a variety of polynomial-time truth-table reductions. Consequences in complexity theory include the definite collapse and (assuming $P \neq PP$) separation of certain query hierarchies over PP. Similar techniques allow us to combine several threshold gates into a single threshold gate. Consequences in the study of circuits include the simulation of circuits with a small number of threshold gates by circuits having only a single threshold gate at the root (perceptrons) and a lower bound on the number of threshold gates that are needed to compute the parity function.

*Keywords* : probabilistic Turing machines

*Classification* :

*68Q05 Models of computation

---

**Zbl 0808.68060**

**Feigenbaum, Joan**; **Fortnow, Lance**; **Lund, Carsten**; **Spielman, Daniel**

**The power of adaptiveness and additional queries in random-self- reductions.** (English)

Comput. Complexity 4, No.2, 158-174 (1994). ISSN 1016-3328; ISSN 1420-8954

http://dx.doi.org/10.1007/BF01202287

http://link.springer.de/link/service/journals/00037/

Summary: We study random-self-reductions from a structural complexity-theoretic point of view. Specifically, we look at relationships between adaptive and nonadaptive random-self-reductions. We also look at what happens to random-self-reductions if we restrict the number of queries they are allowed to make. We show the following results: There exists sets that are adaptively random-self-reducible but not nonadaptively random-self- reducible. Under plausible assumptions, there exist such sets in NP.

There exists a function that has a nonadaptive $(k(n) + 1)$-random-self- reduction but does not have an adaptive $k(n)$-random-self-reduction.
For any countable class of functions $\mathcal{C}$ and any unbounded function $k(n)$, there exists a function that is nonadaptively $k(n)$- uniformly-random-self-reducible but is not in $\mathcal{C}$/poly. This should be contrasted with Feigenbaum, Kannan, and Nisan's theorem that all nonadaptively 2-uniformly-random-self-reducible sets are in NP/poly.

*Keywords* : adaptiveness; random-self-reducibility
*Classification* :
∗68Q15 Complexity classes of computation