Bibliography of Theoretical Computer Science, KTH 2000–2007

April 8, 2008

References

[1] Louigi Addario-Berry, Benny Chor, Michael T. Hallett, Jens Lagergren, Alessandro Panconesi, and Todd Wareham. Ancestral maximum likelihood of evolutionary trees is hard. In *Algorithms in Bioinformatics, Third International Workshop, WABI 2003, Budapest, Hungary, September 15-20, 2003, Proceedings*, pages 202–215, 2003.

[2] Louigi Addario-Berry, Michael T. Hallett, and Jens Lagergren. Towards identifying lateral gene transfer events. In *Pacific Symposium on Biocomputing*, pages 279–290, 2003.

[3] Ben Adida and Douglas Wikström. How to shuffle in public. In *Theory of Cryptography, 4th Theory of Cryptography Conference (TCC)*, pages 555–574, 2007.

[4] Ben Adida and Douglas Wikström. Offline/online mixing. In *Automata, Languages and Programming, 34th International Colloquium (ICALP)*, pages 484–495, 2007.

[5] I. Aktug and D. Gurov. State space representation for verification of open systems. In *Proc. AMAST'06*, volume 4019 of *Lecture Notes in Computer Science*, pages 5–20. Springer, 2006.

[6] I. Aktug and K. Naliuka. Conspec: A formal language for policy specification. In *First Workshop on Formal Languages and Analysis of Contract-Oriented Software*, October 2007.

[7] Wynand B.L. Alkema, Öjvind Johansson, Jens Lagergren, and Wyeth W. Wasserman. MSCAN: identification of functional clusters of transcription factor binding sites. *Nucleic Acids Res*, 32(Web Server issue):W195–8, 2004.

[8] A. Andersson, T. Hagerup, J. Håstad, and O. Petersson. Tight bounds for searching a sorted array of strings. *SIAM J. on Computing*, pages 1552–1578, 2001.

[9] G. Andersson, L. Engebretsen, and J. Håstad. A new way to use semidefinite programming with applications to linear equations mod p. *Journal of Algorithms*, 39:162–204, 2001.

[10] S. Arnborg, I. Agartz, M. Nordström, H. Hall, and G. Sedvall. Human Brain Informatics: Understanding causes of mental illness. *ERCIM News*, pages 24–25, Oct 2000. http://www.ercim.org/publication/.

[11] S. Arnborg and G. Sjödin. On the foundations of Bayesianism. In Ali Mohammad-Djarafi, editor, *Bayesian Inference and Maximum Entropy Methods in Science and Engineering, 20th International Workshop, Gif-sur-Yvette, 2000*, pages 61–71. American Institute of Physics, 2001.

[12] Stefan Arnborg. Robust Bayesianism: Imprecise and paradoxical reasoning. In Per Svensson and Johan Schubert, editors, *Proceedings of the Seventh International Conference on Information Fusion*, volume I, pages 407–414, Mountain View, CA, Jun 2004. International Society of Information Fusion.

[13] Stefan Arnborg. Robust Bayesianism: Relation to Evidence Theory. *ISIF Journal of Advances in Information Fusion*, 1(1):75–90, 2006.

[14] Stefan Arnborg, Ingrid Agartz, Håkan Hall, Erik Jönsson, Anna Sillén, and Göran Sedvall. Data mining in schizophrenia research - preliminary analysis. In *Principles of Data Mining and Knowledge Discovery, 6th European Conference, PKDD 2002, Helsinki, Finland, August 19-23, 2002, Proceedings*, pages 27–38, 2002.

[15] Stefan Arnborg, Henrik Artman, Joel Brynielsson, and Klas Wallenius. Information awareness in command and control: Precision, quality, utility. In *Proceedings of the Third International Conference on Information Fusion (FUSION 2000)*, pages ThB1/25–32, Paris, France, July 2000.

[16] Stefan Arnborg and Gunnar Sjödin. Bayes rules in finite models. In *ECAI 2000, Proceedings of the 14th European Conference on Artificial Intelligence, Berlin, Germany, August 20-25, 2000*, pages 571–575, 2000.

[17] L. Arvestad, A.C. Berglund, J. Lagergren, and B. Sennblad. Bayesian gene/species tree reconciliation and orthology analysis using MCMC. *Bioinformatics*, 19 Suppl 1:i7–15, 2003.

[18] Lars Arvestad, Ann-Charlotte Berglund, Jens Lagergren, and Bengt Sennblad. Bayesian gene/species tree reconciliation and orthology analysis using MCMC. In *Proceedings of the Eleventh International Conference on Intelligent Systems for Molecular Biology, June 29 - July 3, 2003, Brisbane, Australia (Supplement of Bioinformatics)*, pages 7–15, 2003.

[19] Lars Arvestad, Ann-Charlotte Berglund, Jens Lagergren, and Bengt Sennblad. Gene tree reconstruction and orthology analysis based on an integrated model for duplications and sequence evolution. In *Proceedings of the Eighth Annual International Conference on Computational Molecular Biology, 2004, San Diego, California, USA, March 27-31, 2004*, pages 326–335, 2004.

[20] Lars Arvestad, Ann-Charlotte Berglund, Jens Lagergren, and Bengt Sennblad. Gene tree reconstruction and orthology analysis based on an integrated model for duplications and sequence evolution. In *RECOMB '04: Proceedings of the eighth annual international conference on Resaerch in computational molecular biology*, pages 326–335, New York, NY, USA, 2004. ACM Press.

[21] Y. Aumann, J. Håstad, M. Rabin, and M. Sudan. Linear consistency testing. *Journal of Computer and System Sciences*, 62:589–607, 2001.

[22] Per Austrin. Balanced Max 2-Sat might not be the hardest. Technical report, Electronic Colloquium on Computational Complexity Report TR06-088, 2006.

[23] Per Austrin. Balanced Max 2-Sat Might Not be the Hardest. In *ACM Symposium on Theory of Computing (STOC)*, pages 189–197, 2007.

[24] Per Austrin. Towards Sharp Inapproximability For Any 2-CSP. In *IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 307–317, 2007.

[25] R. Bakhshi and D. Gurov. Verification of peer-to-peer algorithms: A case study. In *Proc. MTCoord'06*, Electronic Notes in Theoretical Computer Science, 2006.

[26] Rana Bakhshi and Dilian Gurov. Verification of peer-to-peer algorithms: A case study. *Electr. Notes Theor. Comput. Sci.*, 181:35–47, 2007.

[27] Boaz Barak, Ran Canetti, Yehuda Lindell, Rafael Pass, and Tal Rabin. Secure computation without authentication. In *Advances in Cryptology - CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005, Proceedings*, pages 361–377, 2005.

[28] Boaz Barak, Ran Canetti, Jesper Buus Nielsen, and Rafael Pass. Universally composable protocols with relaxed set-up assumptions. In *45th Symposium on Foundations of Computer Science (FOCS 2004), 17-19 October 2004, Rome, Italy, Proceedings*, pages 186–195, 2004.

[29] Boaz Barak and Rafael Pass. On the possibility of one-message weak zero-knowledge. In *Theory of Cryptography, First Theory of Cryptography Conference, TCC 2004, Cambridge, MA, USA, February 19-21, 2004, Proceedings*, pages 121–132, 2004.

[30] J. Bigert, V. Kann, O. Knutsson, and J. Sjöbergh. Grammar checking for Swedish second language learners. In *CALL for the Nordic Languages*, volume 30 of *Copenhagen Studies in Language*, pages 33–47. Samfundslitteratur, Copenhagen Business School, 2005.

[31] J. Bigert, O. Knutsson, V. Kann, and J. Sjöbergh. Annotated clauses and flat phrase structures for Swedish. In *Swedish Treebank Symposium*, 2002.

[32] Johnny Bigert, Viggo Kann, Ola Knutsson, and Jonas Sjöbergh. Grammar checking for swedish second lanuage learners. In Peter Juel Henrichsen, editor, *CALL for the Nordic Languages*, pages 33–47. Samfundslitteratur, 2004.

[33] Johnny Bigert, Ola Knutsson, Viggo Kann, and Jonas Sjöbergh. Annotated clauses and flat phrase structures for Swedish, 2002.

[34] Johnny Bigert, Ola Knutsson, and Jonas Sjöbergh. Automatic evaluation of robustness and degradation in tagging and parsing. In *Proceedings of RANLP-2003*, pages 51–57, Borovets, Bulgaria, 2003.

[35] Johnny Bigert, Jonas Sjöbergh, Ola Knutsson, and Magnus Sahlgren. Unsupervised evaluation of parser robustness. In *Proceedings of CICLing 2005*, pages 142–154, Mexico City, Mexico, 2005.

[36] Joel Brynielsson. A decision–theoretic framework using rational agency. In *Proceedings of the 11th Conference on Computer-Generated Forces and Behavioral Representation*, number 02–CGF–047, pages 459–463, Orlando, Florida, May 2002.

[37] Joel Brynielsson. Game-theoretic reasoning in command and control. In *Proceedings of the 15th Mini-EURO Conference: Managing Uncertainty in Decision Support Models (MUDSM 2004)*, Coimbra, Portugal, September 2004.

[38] Joel Brynielsson. Using AI and games for decision support in command and control. *Decision Support Systems*, 43(4):1454–1463, August 2007.

[39] Joel Brynielsson and Stefan Arnborg. Bayesian games for threat prediction and situation analysis. In Per Svensson and Johan Schubert, editors, *Proceedings of the Seventh International Conference on Information Fusion (FUSION 2004)*, volume 2, pages 1125–1132, Stockholm, Sweden, June 28–July 1, 2004.

[40] Joel Brynielsson and Stefan Arnborg. Refinements of the command and control game component. In *Proceedings of the Eighth International Conference on Information Fusion (FUSION 2005)*, Philadelphia, Pennsylvania, July 2005.

[41] Joel Brynielsson and Stefan Arnborg. An information fusion game component. *Journal of Advances in Information Fusion*, 1(2):108–121, December 2006.

[42] Joel Brynielsson, Mattias Engblom, Robert Franzén, Jonas Nordh, and Lennart Voigt. Enhanced situation awareness using random particles. In *Proceedings of the Tenth International Command and Control Research and Technology Symposium (ICCRTS)*, McLean, Virginia, June 2005.

[43] Joel Brynielsson and Rego Granlund. Assistance in decision making: Decision help and decision analysis. In *Proceedings of the Sixth International Command and Control Research and Technology Symposium (ICCRTS)*, Annapolis, Maryland, June 2001.

[44] Joel Brynielsson and Klas Wallenius. Game environment for command and control operations (GECCO). In *Proceedings of the First International Workshop on Cognitive Research With Microworlds*, pages 85–95, Granada, Spain, November 2001.

[45] Joel Brynielsson and Klas Wallenius. A toolbox for multi-attribute decision-making. Technical Report TRITA–NA–0307, Department of Numerical Analysis and Computer Science, Royal Institute of Technology, Stockholm, Sweden, December 2003.

[46] T. Chow, H. Eriksson, and K. Fan. Chess tableaux. *Electronic J. Combinatorics*, 11(2):18 pp., June 2005.

[47] Mika Cohen and Mads Dam. A complete axiomatization of knowledge and cryptography. In *22nd IEEE Symposium on Logic in Computer Science (LICS)*, pages 77–88, 2007.

[48] H. Dalianis, M. Rimka, and V. Kann. Using Uplug and SiteSeeker to construct a cross language search engine for Scandinavian. In *Workshop: The Automatic Treatment of Multilinguality in Retrieval, Search and Lexicography*, April 2007.

[49] Mads Dam. Decidability and proof systems for language-based noninterference relations. In *Proceedings of the 33rd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL 2006, Charleston, South Carolina, USA, January 11-13, 2006*, pages 67–78. ACM, 2006.

[50] S. Djerbi, M. Lindskog, L. Arvestad, F. Sterky, and T.T. Teeri. The genome sequence of black cottonwood (populus trichocarpa) reveals 18 conserved cellulose synthase (cesa) genes. *Planta*, 221(5):739–746, Jul 2005.

[51] Y. Dodis, R. Gennaro, J. Håstad, H. Krawczyk, and T. Rabin. Randomness extraction and key derivation using the CBC cascade and HMAC modes. In M. Franklin, editor, *Proceedings of CRYPTO 2004, LNCS 3152*, pages 494–510, 2004.

[52] D. Dor, J. Håstad, S. Ulfberg, and U. Zwick. On lower bounds for selecting the median. *SIAM Journal on Discrete Mathematics*, 14:299–311, 2001.

[53] Isaac Elias. Settling the intractability of multiple alignment. In *Proc. of the 14th Ann. Int. Symp. on Algorithms and Computation (ISAAC'03)*,

volume 2906 of *Lecture Notes in Computer Science*, pages 352–363. Springer-Verlag, November 2003.

[54] Isaac Elias. Settling the intractability of multiple alignment. Technical Report TRITA-NA-0316, Nada, KTH, 2003.

[55] Isaac Elias and Tzvika Hartman. A 1.375-approximation algorithm for sorting by transpositions. In *Proc. of the 5th International Workshop on Algorithms in Bioinformatics (WABI'05)*, volume 3692 of *Lecture Notes in Computer Science*, pages 204–214. Springer-Verlag, October 2005.

[56] Isaac Elias and Jens Lagergren. Fast neighbor joining. In *Proc. of the 32nd International Colloquium on Automata, Languages and Programming (ICALP'05)*, volume 3580 of *Lecture Notes in Computer Science*, pages 1263–1274. Springer-Verlag, July 2005.

[57] Henrik Eriksson, Kimmo Eriksson, Johan Karlander, Lars J. Svensson, and Johan Wästlund. Sorting a bridge hand. *Discrete Mathematics*, 241(1-3):289–300, 2001.

[58] Kimmo Eriksson and Johan Karlander. Stable matching in a common generalization of the marriage and assignment models. *Discrete Mathematics*, 217(1-3):135–156, 2000.

[59] David Fernández-Baca and Jens Lagergren. A polynomial-time algorithm for near-perfect phylogeny. *SIAM J. Comput*, 32(5):1115–1127, 2003.

[60] Johan Glimming. Parametric (co)iteration vs. primitive direcursion. In *Algebra and Coalgebra in Computer Science, Second International Conference (CALCO)*, pages 257–278, 2007.

[61] Johan Glimming and Neil Ghani. Difunctorial semantics of object calculus. In *Proceedings of the Second Workshop on Object Oriented Developments (WOOD 2004)*, volume 138 of *Electronic Notes in Theoretical Computer Science*, pages 79–94. Elsevier, November 2005.

[62] M. Goldmann, Näslund, and Russell. Complexity bounds on general hard-core predicates. *JCRYPTOL: Journal of Cryptology*, 14, 2001.

[63] M. Goldmann and A. Russell. Spectral bounds on general hard core predicates. In *STACS: Annual Symposium on Theoretical Aspects of Computer Science*, 2000.

[64] M. Goldmann and A. Russell. The complexity of solving equations over finite groups. *INFCTRL: Information and Computation (formerly Information and Control)*, 178, 2002.

[65] M. Goldmann, A. Russell, and Therien. An ergodic theorem for read-once non-uniform deterministic finite automata. *IPL: Information Processing Letters*, 73, 2000.

[66] V. Guruswami, J. Håstad, and M. Sudan. Hardness of approximate hypergraph coloring. In *Proceedings of 41st Annual IEEE Symposium on Foundations of Computer Science*, pages 149–158, 2000.

[67] V. Guruswami, J. Håstad, and M. Sudan. Hardness of approximate hypergraph coloring. *SIAM Journal on Computing*, 31:1663–1686, 2002.

[68] V. Guruswami, J. Håstad, M. Sudan, and D. Zuckerman. Combinatorial bounds for list decoding. In *38th Annual Allerton Conference of Communication, Control and Computing*, 2000.

[69] V. Guruswami, J. Håstad, M. Sudan, and D. Zuckerman. Combinatorial bounds for list decoding. *IEEE Transactions on Information Theory*, pages 1021–1034, 2002.

[70] H. Hall, G. Lawyer, A. Sillen, EG Jönsson, I. Agartz, L. Terenius, and S. Arnborg. Potential genetic variants in schizophrenia: A Bayesian analysis. *World J Biol Psychiatry*, 8(1):12–22, 2007.

[71] M. T. Hallett and J. Lagergren. New algorithms for the duplication-loss model. In Ron Shamir, Satoru Miyano, Sorin Istrail, Pavel Pevzner, and Michael Waterman, editors, *Proceedings of the 4th Annual International Conference on Computational Molecular Biology (RECOMB-00)*, pages 138–146, N.Y., April 8–11 2000. ACM Press.

[72] Michael T. Hallett and Jens Lagergren. Hunting for functionally analogous genes. In *Foundations of Software Technology and Theoretical Computer Science, 20th Conference, FST TCS 2000 New Delhi, India, December 13-15, 2000, Proceedings.*, pages 465–476, 2000.

[73] Michael T. Hallett and Jens Lagergren. Efficient algorithms for lateral gene transfer problems. In Thomas Lengauer, David Sankoff, Sorin Istrail, Pavel Pevzner, and Michael Waterman, editors, *Proceedings of the Fith International Conference on Computational Biology (RECOMB-01)*, pages 149–156, New York, April 22–25 2001. ACMPress.

[74] Michael T. Hallett, Jens Lagergren, and Ali Tofigh. Simultaneous identification of duplications and lateral transfers. In *Proceedings of the Eighth Annual International Conference on Computational Molecular Biology, 2004, San Diego, California, USA, March 27-31, 2004*, pages 347–356, 2004.

[75] Martin Hassel and Jonas Sjöbergh. A reflection of the whole picture is not always what you want, but that is what we give you. In *"Crossing Barriers in Text Summarization Research" workshop at RANLP'05*, Borovets, Bulgaria, 2005.

[76] Martin Hassel and Jonas Sjöbergh. Towards holistic summarization: Selecting summaries, not sentences. In *Proceedings of LREC 2006*, Genoa, Italy, 2006.

[77] J. Håstad. On bounded occurrence constraint satisfaction. *Information Processing Letters*, 74:1–6, 2000.

[78] J. Håstad. Which NP-hard optimization problems admit non-trivial efficient approximation algorithms. In *Proceedings of ICALP 2000 (invited presentation), LNCS 1853*, pages 235–235, 2000.

[79] J. Håstad. A slight sharpening of LMN. *Journal of Computer and System Sciences*, 63:498–508, 2001.

[80] J. Håstad. Some optimal inapproximability results. *Journal of ACM*, 48:798–859, 2001.

[81] J. Håstad. Inapproximability-some history and some open problems. In *Proceedings of the 18th Annual IEEE conference on Computational Complexity*, pages 265–266, 2003.

[82] J. Håstad. Every 2-CSP allows nontrivial approximation. In *Proceedings of the 37th Annual ACM Symposium on Theory of Computation*, pages 740–746, 2005.

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

[84] J. Håstad, J. Jonsson, A. Juels, and M. Yung. Funkspiel schemes: An alternative to conventional tamper resistance. In S. Jajodia and P. Samarati, editors, *Proceedings of the 7th ACM Conference on Computer Communications Security*, pages 125–133, 2000.

[85] J. Håstad and S. Khot. Query efficient PCPs with perfect completeness. In *Proceedings of 42nd Annual IEEE Symposium on Foundations of Computer Science*, pages 610–619, 2001.

[86] J. Håstad and S. Khot. Query efficient PCPs with perfect completeness. *Theorey of Computing*, 1:119–149, 2005.

[87] J. Håstad, S. Linusson, and J.Wästlund. A smaller sleeping bag for a baby snake. *Discrete and Computational Geometry*, pages 173–181, 2001.

[88] J. Håstad and M. Näslund. BMGL: Synchronous key-stream generator with provable security. In *Proceedings of the 1st Open NESSIE Workshop*, 2000.

[89] J. Håstad and M. Näslund. Practical construction and analysis of pseudo-randomness primitives. In *Advances in Cryptology—Asiacrypt 2001,LNCS 2248*, pages 442–459, 2001.

[90] J. Håstad and M. Näslund. The security of all RSA and discrete log bits. *Journal of the ACM*, 51:187–230, 2004.

[91] J. Håstad and V. Srinivasan. On the advantage over a random assignment. In *Proceedings of the 34th Annual ACM Symposium on Theory of Computation*, pages 43–52, 2002.

[92] J. Håstad and V. Srinivasan. On the advantage over a random assignment. *Random structures and Algorithms*, 25:117–149, 2004.

[93] J. Håstad and A. Wigderson. Simple analysis of graph tests for linearity and PCP. *Random Structures and algorithms*, 22:139–160, 2003.

[94] J. Håstad and Avi Wigderson. Simple analysis of graph tests for linearity and PCP. In *Proc. of Conference on Computational Complexity*, pages 244–255, 2001.

[95] Johan Håstad. The square lattice shuffle. *Random Struct. Algorithms*, 29(4):466–474, 2006.

[96] Johan Håstad. On the approximation resistance of a random predicate. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, 10th International Workshop, APPROX 2007, and 11th International Workshop, (APPROX-RANDOM)*, pages 149–163, 2007.

[97] Johan Håstad. The security of the IAPM and IACBC modes. *J. Cryptology*, 20(2):153–163, 2007.

[98] Johan Håstad and Mikael Goldmann. Majority gates vs. general, April 09 2004.

[99] Johan Håstad, Lars Ivansson, and Jens Lagergren. Fitting points on the real line and its application to RH mapping. *J. Algorithms*, 49(1):42–62, 2003.

[100] V. Hollich, L. Milchert, L. Arvestad, and E.L. Sonnhammer. Assessment of protein distance measures and tree-building methods for phylogenetic tree reconstruction. *Mol Biol Evol*, 22(11):2257–2264, Nov 2005.

[101] Qi Huang, Jenny Hållmats, Klas Wallenius, and Joel Brynielsson. Simulation-based decision support for command and control in joint operations. In *Proceedings of the 2003 European Simulation Interoperability Workshop*, number 03E–SIW–091, pages 591–599, Stockholm, Sweden, June 2003.

[102] J. Håstad. The security of the IAPM and IACBC modes. *Journal of Cryptology*, 2006.

[103] J. Håstad and A. Wigderson. The randomized communication complexity of set disjointness. *Theory of Computing*, 3:211–219, 2007.

[104] Johan Håstad. On the efficient approximability of constraint satisfaction problems. In *Surveys in Combinatorics*, volume 346. London Mathematical Society, 2007.

[105] Lars Ivansson and Jens Lagergren. Algorithms for RH mapping: New ideas and improved analysis. *SIAM Journal on Computing*, 34(1):89–108, February 2005.

[106] Mattias Johansson, Gunnar Kreitz, and Fredrik Lindholm. Stateful subset cover. *Lecture Notes in Computer Science*, 3989:178–193, 2006.

[107] Ö. Johansson. MSCAN source code, September 2004.

[108] Ö. Johansson, W. Alkema, W. W. Wasserman, and J. Lagergren. Identification of functional clusters of transcription factor binding motifs in genome sequences: the MSCAN algorithm. *Bioinformatics*, 19(Suppl. 1):i169–76, 2003.

[109] Öjvind Johansson. *Graph Decomposition Using Node Labels*. PhD thesis, Royal Institute of Technology, Stockholm, 2001.

[110] Öjvind Johansson. $\log n$-Approximative NLC_k-decomposition in $O(n^{2k+1})$ time. In *Proc. 27th Int. Workshop on Graph-Theoretic Concepts in Computer Science*, volume 2204 of *Lecture Notes in Computer Science*, pages 229–240, Berlin, 2001. Springer.

[111] Öjvind Johansson, Wynand Alkema, Wyeth W. Wasserman, and Jens Lagergren. Identification of functional clusters of transcription factor binding motifs in genome sequences: the MSCAN algorithm. In *Proceedings of the Eleventh International Conference on Intelligent Systems for Molecular Biology, June 29 - July 3, 2003, Brisbane, Australia (Supplement of Bioinformatics)*, pages 169–176, 2003.

[112] V. Kann, R. Domeij, J. Hollman, and M. Tillenius. Implementation aspects and applications of a spelling correction algorithm. In L. Uhlirova, G. Wimmer, G. Altmann, and R. Koehler, editors, *Text as a Linguistic Paradigm: Levels, Constituents, Constructs. Festschrift in honour of Ludek Hrebicek*, volume 60 of *Quantitative Linguistics*, pages 108–123. WVT, Trier, Germany, 2001.

[113] V. Kann and M. Rosell. Free construction of a Swedish dictionary of synonyms. In *Proc. 15th Nordic Conf. on Computational Linguistics*, 2005.

[114] Viggo Kann. Målrelaterade betygskriterier kräver modifierad examination - examination efter betygskriterier i en algoritmkurs på kth (in swedish). In *Högskoleverkets kvalitetskonferens*, October 2007.

[115] Viggo Kann and J. Hollman. Tvärslå - defining an XML exchange format and then building an on-line nordic dictionary. In *Workshop: The Automatic Treatment of Multilinguality in Retrieval, Search and Lexicography*, April 2007.

[116] O. Knutsson, J. Bigert, and V. Kann. A robust shallow parser for Swedish. In *Proc. 14th Nordic Conf. on Computational Linguistics*, 2003.

[117] O. Knutsson, J. Carlberger, and V. Kann. An object-oriented rule language for high-level text processing. In *Proc. 13th Nordic Conf. on Computational Linguistics*, 2001.

[118] Jens Lagergren. Combining polynomial running time and fast convergence for the disk-covering method. *J. Comput. Syst. Sci*, 65(3):481–493, 2002.

[119] Jens Lagergren and Lars Ivansson. A 7/3-approximation algorithm for fitting points on the real line and its application to RH mapping, December 01 2000.

[120] Glenn Lawyer, Håkan Nyman, Ingrid Agartz, Stefan Arnborg, Erik G Jönsson, Göran C Sedvall, and Håkan Hall. Morphological correlates to cognitive dysfunction in schizophrenia as studied with Bayesian regression. *BMC Psychiatry*, 6(31), 2006.

[121] Karl Meinke. Validation and test case generations for MSCs using A propositional SAT solver. In *SAM 2000, 2nd Workshop on SDL and MSC, Col de Porte, Grenoble, France, June 26-28, 2000*, page 203, 2000.

[122] Karl Meinke. Proof theory of higher-order equations: conservativity, normal forms and term rewriting. *J. Comput. Syst. Sci*, 67(1):127–173, 2003.

[123] Karl Meinke. Automated black-box testing of functional correctness using function approximation. In *Proceedings of the ACM/SIGSOFT International Symposium on Software Testing and Analysis, ISSTA 2004, Boston, Massachusetts, USA, July 11-14, 2004*, pages 143–153, 2004.

[124] Karl Meinke. A stochastic theory of black-box software testing. In Kokichi Futatsugi, Jean-Pierre Jouannaud, and José Meseguer, editors, *Algebra, Meaning, and Computation, Essays Dedicated to Joseph A. Goguen on the Occasion of His 65th Birthday*, volume 4060 of *Lecture Notes in Computer Science*, pages 578–595. Springer, 2006.

[125] Karl Meinke. Iterative estimators of parameters in linear models with partially variant coefficients. *the International Journal of Applied Mathematics and Computer Science*, to appear, 2007.

[126] Karl Meinke and L. J. Steggles. Correctness of dataflow and systolic algorithms using algebras of streams. *Acta Inf*, 38(1):45–88, 2001.

[127] Jakob Nordström. Narrow proofs may be spacious: Separating space and width in resolution. *Electronic Colloquium on Computational Complexity (ECCC)*, 066(066), 2005.

[128] Jakob Nordström. Narrow proofs may be spacious: Separating space and width in resolution (extended abstract). In *Proceedings 38th Annual ACM Symposium on Theory of Computing (STOC '06)*, pages 507–516, May 2006.

[129] Jakob Nordström. Narrow proofs may be spacious: Separating space and width in resolution. Technical Report TR05-066, Revision 02, Electronic Colloquium on Computational Complexity (ECCC), November 2005.

[130] Robert Olsson and Stefan Nilsson. TRASH - a dynamic LC-trie and hash data structure. Technical Report Trita–CSC–TCS 2006:2, School of Computer Science and Communication, Royal Institute of Technology, Stockholm, Sweden, December 2006.

[131] Robert Olsson and Stefan Nilsson. Trash - a dynamic lc-trie and hash data structure. In *IEEE 2007 Workshop on High Performance Switching and Routing (HPSR2007)*. Polytechnic University, Brookly, NY, 2007.

[132] Roland Orre, Andrew Bate, G. Niklas Norén, Erik Swahn, Stefan Arnborg, and I. Ralph Edwards. A bayesian recurrent neural network for unsupervised pattern recognition in large incomplete data sets. *Int. J. Neural Syst*, 15(3):207–222, 2005.

[133] Anna Palbom. Complexity of the directed spanning cactus problem. *Discrete Applied Mathematics*, 146:81–91, 2005.

[134] Rafael Pass. On deniability in the common reference string and random oracle model. In *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings*, pages 316–337, 2003.

[135] Rafael Pass. Simulation in quasi-polynomial time, and its application to protocol composition. In *Advances in Cryptology - EUROCRYPT 2003, International Conference on the Theory and Applications of Cryptographic Techniques, Warsaw, Poland, May 4-8, 2003, Proceedings*, pages 160–176, 2003.

[136] Rafael Pass. Bounded-concurrent secure multi-party computation with a dishonest majority. In *Proceedings of the thirty-sixth annual ACM Symposium on Theory of Computing (STOC-04)*, pages 232–241, New York, June 13–15 2004. ACM Press.

[137] Rafael Pass and Alon Rosen. Bounded-concurrent secure two-party computation in a constant number of rounds. In *44th Symposium on Foundations of Computer Science (FOCS 2003), 11-14 October 2003, Cambridge, MA, USA, Proceedings*, page 404, 2003.

[138] Rafael Pass and Alon Rosen. Concurrent non-malleable commitments. In *46th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2005), 23-25 October 2005, Pittsburgh, PA, USA, Proceedings*, pages 563–572, 2005.

[139] Rafael Pass and Alon Rosen. New and improved constructions of non-malleable cryptographic protocols. In *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, May 22-24, 2005*, 2005.

[140] Rafael Pass and Abhi Shelat. Unconditional characterizations of non-interactive zero-knowledge. In *Advances in Cryptology - CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005, Proceedings*, pages 118–134, 2005.

[141] M. Rosell. Improving clustering of Swedish newspaper articles using stemming and compound splitting. In *Proc. 14th Nordic Conf. on Comp. Ling. – NODALIDA '03*, 2003.

[142] M. Rosell, V. Kann, and J. Litton. Comparing comparisons: Document clustering evaluation using two manual classifications. In *Proc. Int. Conf. on Natural Language Processing (ICON – 2004)*, pages 207–216. Allied Publishers Pvt. Ltd., 2004.

[143] M. Rosell and S. Velupillai. The impact of phrases in document clustering for Swedish. In *Proc. 15th Nordic Conf. on Comp. Ling. – NODALIDA '05*, 2005.

[144] Alon Rosen and Rafael Pass. Bounded-concurrent secure two-party computation, September 05 2003.

[145] P. Savolainen, C. Fitzsimmons, L. Arvestad, L. Andersson, and J. Lundeberg. ESTs from brain and testis of white leghorn and red junglefowl: annotation, bioinformatic classification of unknown transcripts and analysis of expression levels. *Cytogenet Genome Res*, 111(1):79–87, 2005.

[146] K. Shiv, R. Iyer, C. Newburn, J. Dahlstedt, M. Lagergren, and O. Lindholm. Impact of JIT/JVM optimizations on java application performance. In *7th Annual Workshop on Interaction between Compilers and Computer Architecture (INTERACT-7 2003), 8 February 2003, Anaheim, CA, USA*, pages 5–13, 2003.

[147] J. Sjöbergh and V. Kann. Finding the correct interpretation of Swedish compounds, a statistical approach. In *Proc. 4th Int. Conf. Language Resources and Evaluation (LREC 2004)*, 2004.

[148] J. Sjöbergh and V. Kann. Vad kan statistik avslöja om svenska sammansättningar? *Språk och stil*, 16, 2006.

[149] Jonas Sjöbergh. Bootstrapping a free part-of-speech lexicon using a proprietary corpus. In *Proceedings of ICON-2003: International Conference on Natural Language Processing*, pages 1–8, Mysore, India, 2003.

[150] Jonas Sjöbergh. Combining pos-taggers for improved accuracy on Swedish text. In *Proceedings of NoDaLiDa 2003*, Reykjavik, Iceland, 2003.

[151] Jonas Sjöbergh. Stomp, a POS-tagger with a different view. In *Proceedings of RANLP-2003*, pages 440–444, Borovets, Bulgaria, 2003.

[152] Jonas Sjöbergh. Chunking: an unsupervised method to find errors in text. In *Proceedings of NODALIDA 2005*, Joensuu, Finland, 2005.

[153] Jonas Sjöbergh. Creating a free digital Japanese-Swedish lexicon. In *Proceedings of PACLING 2005*, pages 296–300, Tokyo, Japan, 2005.

[154] Jonas Sjöbergh. The internet as a normative corpus: Grammar checking with a search engine. Technical Report TRITA-CSC-TCS 2006:3, School of Computer Science and Communication, the Royal Institute of Technology, Stockholm, Sweden, 2006.

[155] Jonas Sjöbergh. Vulgarities are fucking funny, or at least make things a little bit funnier. Technical Report TRITA-CSC-TCS 2006:4, School of Computer Science and Communication, the Royal Institute of Technology, Stockholm, Sweden, 2006.

[156] Jonas Sjöbergh and Kenji Araki. Extraction based summarization using a shortest path algorithm. In *Proceedings of the 12th Annual Natural Language Processing Conference NLP2006*, pages 1071–1074, Yokohama, Japan, 2006.

[157] Jonas Sjöbergh and Viggo Kann. Finding the correct interpretation of Swedish compounds a statistical approach. In *Proceedings of LREC-2004*, pages 899–902, Lisbon, Portugal, 2004.

[158] Jonas Sjöbergh and Ola Knutsson. Faking errors to avoid making errors: Very weakly supervised learning for error detection in writing. In *Proceedings of RANLP 2005*, pages 506–512, Borovets, Bulgaria, 2005.

[159] R. Suzic. A generic model of plan recognition using embedded simulations, microeconomics and behavior models. In *Proc. BRIMS 2006*, 2006.

[160] R. Suzic and P. Svensson. Capabilities-based plan recognition. In *Proc. FUSION 2006*, 2006.

[161] M. Trolin. On the security of non-RSA EMV payment cards. In *EUROMEDIA 2005*, 2005.

[162] M. Trolin. A universally composable scheme for electronic cash. In *Advances in Cryptology – INDOCRYPT 2005*, volume 3797 of *Lecture Notes in Computer Science*, pages 347 – 360. Springer Verlag, 2005. Full version at `http://eprint.iacr.org/2005/341`.

[163] M. Trolin and D. Wikström. Hierarchical group signatures. In *International Colloquium on Automata, Languages and Programming – ICALP 2005*, volume 3580 of *Lecture Notes in Computer Science*, pages 446 – 458. Springer Verlag, 2005. Full version at `http://eprint.iacr.org/2004/311`.

[164] Rand Waltzman, Kristina Winbladh, Thomas A. Alspaugh, and Debra J. Richardson. In the requirements lies the power. In *SEKE*, pages 185–190, 2007.

[165] Douglas Wikström. On the l -ary GCD-algorithm in rings of integers. In Luís Caires, Giuseppe F. Italiano, Luís Monteiro, Catuscia Palamidessi, and Moti Yung, editors, *Automata, Languages and Programming, 32nd International Colloquium, ICALP 2005, Lisbon, Portugal, July 11-15, 2005, Proceedings*, volume 3580 of *Lecture Notes in Computer Science*, pages 1189–1201. Springer, 2005.

[166] Douglas Wikström. A sender verifiable mix-net and a new proof of a shuffle. In Bimal K. Roy, editor, *Advances in Cryptology - ASIACRYPT 2005, 11th International Conference on the Theory and Application of Cryptology and Information Security, Chennai, India, December 4-8,*

2005, Proceedings, volume 3788 of *Lecture Notes in Computer Science*, pages 273–292. Springer, 2005.

[167] Douglas Wikström. Designated confirmer signatures revisited. In *Theory of Cryptography, 4th Theory of Cryptography Conference (TCC)*, pages 342–361, 2007.

[168] Fetahi Wuhib, Mads Dam, Rolf Stadler, and Alexander Clemm. Robust monitoring of network-wide aggregates through gossiping. In *Integrated Network Management*, pages 226–235, 2007.