Bibliography of Theoretical Computer Science, KTH 2005

September 6, 2006

References

[1] Boaz Barak, Ran Canetti, Yehuda Lindell, Rafael Pass, and Tal Rabin. Secure computation without authentication. In Victor Shoup (Ed), editor, *Advances in Cryptology - CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005, Proceedings*, volume 3621 of *Lecture Notes in Computer Science*, pages 361–377. Springer, 2005.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

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

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

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

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

[14] 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.

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

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

[17] 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.

[18] 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.

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

[20] 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. IEEE Computer Society, 2005.

[21] Rafael Pass and Alon Rosen. New and improved constructions of non-malleable cryptographic protocols. In Harold N. Gabow and Ronald Fagin, editors, *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, May 22-24, 2005*, pages 533–542. ACM, 2005.

[22] Rafael Pass and Abhi Shelat. Unconditional characterizations of non-interactive zero-knowledge. In Victor Shoup (Ed), editor, *Advances in Cryptology - CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005, Proceedings*, volume 3621 of *Lecture Notes in Computer Science*, pages 118–134. Springer, 2005.

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

[24] 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.

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

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

[27] 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.

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

[29] 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`.

[30] 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`.

[31] 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, *ICALP*, volume 3580 of *Lecture Notes in Computer Science*, pages 1189–1201. Springer, 2005.

[32] Douglas Wikström. A sender verifiable mix-net and a new proof of a shuffle. In Bimal K. Roy, editor, *ASIACRYPT*, volume 3788 of *Lecture Notes in Computer Science*, pages 273–292. Springer, 2005.