

CURRICULUM VITAE

Stefan Wegenkittl
Salzburg, August, 2007



Personal Data

Name	Univ. Doz. Dr. Mag. Rer. Nat. Stefan Wegenkittl
Birth	July 8, 1969, Salzburg

Education

1975–1987	primary and secondary school at Salzburg
Jun. 11, 1987	Matura (with excellence)
1988–1995	study of Mathematics (with emphasis on Statistics and Probability Theory) and Computer Sciences, Salzburg
Dec. 14, 1995	Master's Degree in Mathematics with excellence
Jul. 10, 1998	PhD. in Mathematics with excellence
Jul. 4, 2004	Habilitation at the Department for Mathematics, University Salzburg

Research Experience

Mathematical Statistics, Stochastic Modelling and Simulation, Analysis of Stochastic Processes (Hidden Markov Models), Stochastic Image Analysis (Segmentation, Coregistration), Pattern Recognition and Data Clustering for Gene Hunting, Random Number Generation and Cryptography, Performance Analysis for Stochastic Algorithms, Neural Networks and Genetic Algorithms, High Performance Computing, Metric Number Theory

Professional Activities, Management and Organization

Since 2003	Professorship for Mathematics and Informatics at the Salzburg University of Applied Sciences
1999-2003	Manager of applied mathematics (SRS Medizintechnik and ProCeryon Biosciences)
1995-1999	Research assistant (Dep. of Mathematics, University of Salzburg)

Other activities:

Technical project management for KPlus, FWF, FFF and EU proposals and projects (ISM Austria, ProCeryon Biosciences, and University)
Software engineering and system/network management (Graber Taschwer Software, SPC Computerschulung, and Keywi-Music)

Honors and Awards

- 1988–1993 Österreichisches Begabtenstipendium (2 times)
- 1995 Förderungspreis d. Inst. f. Mathematik der Universität Salzburg

Selected Projects

- 2003– Development of graphical tools for quality management in coronary surgery. Cooperation with Dr. R. Schistek (SALK Salzburger Landeskliniken)
- 2001–2002 Manager of Applied Mathematics, SRS Medizintechnik GmbH, Austria. Development of a simulator for neurosurgery. Mathematical modelling for elastodynamics and computational fluid simulation, stochastic image analysis for semi-automatic segmentation and coregistration of MR and CT scans.
- 1999–2001 Manager of Bioinformatics and Applied Mathematics, ProCeryon Biosciences GmbH, Austria. Automated genome annotation by combining sequence- and structure-based methods to improve sensitivity and specificity, performance analysis of combined scores using neural networks.
- 1995–2003 CEI-PACT and FWF research assistant at the Dept. of Mathematics at the University of Salzburg. Introduction and mathematical analysis of a generalized ϕ -divergence, distance measures for probability measures, analysis of Markov models, design of empirical tests for pseudorandom number generators, parallel stochastic simulation and empirical testing, CEI-PACT Projekt WP5.1, FWF-Grants P11143/Mat, P13480/Mat, and S8303 at the Dept. of Mathematics in Salzburg, proposed by Ao.Univ.Prof.Dr.Peter Hellekalek.
- 1996– Structural analysis of inversive pseudorandom numbers in collaboration with Doz. Dr. Jürgen Eichenauer–Herrmann of the University of Darmstadt. Number theoretic description of the hyperbola structures in the set of overlapping pairs.
- 1996– PMCI project: implementation and statistical analysis of a software package for parallel pseudorandom number generation. Design and implementation of the scheduling mechanism (task-lists), intense numerical analysis of the quality of the parallel streams of pseudorandom numbers together with Dr. K. Entacher und Dr. A. Uhl.
- 1992–1994 Integration of genetic algorithms in an object oriented development tool for neural computing, ECANSE. Mathematical modelling, software analysis and design. Cooperation of the University of Salzburg and Siemens Wien under the guidance of Prof.Dr. Zinterhof.
- 1997– Analysis of the distribution of the distance of atoms by stochastic simulation and numerical integration in cooperation with Ao.Univ.Prof.Dr. Manfred Sippl, CAME (Center of Applied Molecular Engineering).
- 1997 More-dimensional nonlinear regression: data analysis and graphical presentation for the project “Soziales Netzwerk, Soziale Unterstützung, Soziale Belastung und Befindlichkeit” of O.Prof.Dr. Urs Baumann.

Courses at the University

From 1994 on I held the following courses at the Dept. of Mathematics and Dept. of Scientific Computing, University of Salzburg: lectures (Markov Chains), seminars (analysis I, discrete mathematics, stochastic modeling, programming in C, mathematical software), tutorials (analysis I and II, discrete mathematics). Since 2002 I held courses on Mathematics, Pattern Recognition and Cryptology at Salzburg University of Applied Sciences in the degree program Information Technology and Systems Management and supervised numerous Master's theses on related topics.

Other Professions

- 2002– Member of Advisory Board of PDH International (www.pdhint.com)
- 1990–1991 Software development and ADA-compiler tests for Graber-Taschwer Software, Salzburg.
- 1989–1991 Software trainer for Unix/Xenix, SPC Computerschulung Salzburg.
- 1991–1995 Windows NT/Novell/Win95 LAN installation, administration and system management, Keywi-Music, Salzburg.
- 1989–1995 Studienkommission Mathematik, Studienrichtungsvertretung Mathematik and Computerwissenschaften.

Publications

Theses

- [1] S. Wegenkittl. *Entropy and Divergence Statistics for Markovian Processes and Related Structural and Statistical Properties of Pseudorandom Number Generators*. Habilitation thesis, Universität Salzburg, Österreich, 2003.
- [2] S. Wegenkittl. *Generalized ϕ -Divergence and Frequency Analysis in Markov Chains*. PhD thesis, Universität Salzburg, Österreich, 1998. HTML version: <http://random.mat.sbg.ac.at/~ste/diss>.
- [3] S. Wegenkittl. Empirical testing of pseudorandom number generators. Master's thesis, Universität Salzburg, Österreich, 1995. HTML version: <http://random.mat.sbg.ac.at/~ste/dipl>.

Papers in Scientific Journals

- [4] Peter Hellekalek and Stefan Wegenkittl. Empirical evidence concerning AES. *ACM Trans. Model. Comput. Simul.*, 13(4):322–333, 2003.
- [5] S. Wegenkittl. A generalized ϕ -divergence for asymptotically multivariate normal models. *Journal of Multivariate Analysis*, 83:288–302, 2002.
- [6] S. Wegenkittl. Entropy estimators and serial tests for ergodic chains. *IEEE Transactions on Information Theory*, 47(6):2480–2489, Sep 2001.
- [7] S. Wegenkittl. Gambling tests for pseudorandom number generators. *Mathematics and Computers in Simulation*, 55(1–3):281–288, 2001.
- [8] T. Schell and S. Wegenkittl. Looking beyond selection probabilities: adaption of the χ^2 measure for the performance analysis of selection methods in GA. *Evolutionary*

Computation, MIT Press, 9(2):243–256, 2001.

- [9] P. L’Ecuyer, R. Simard, and S. Wegenkittl. Sparse Serial Tests of Uniformity for Random Number Generators. *SIAM Journal on Scientific Computing*, **24**(2):652–668, 2002.
- [10] S. Wegenkittl and M. Matsumoto. Getting rid of correlations among pseudorandom numbers: Discarding versus tempering. *ACM Trans. Modeling and Computer Simulation*, **9**(3):282–294, 1999.
- [11] S. Wegenkittl. Are there hyperbola in the scatter plots of inversive congruential pseudorandom numbers? *J. Computational And Applied Mathematics*, **95**(1-2):117–125, 1998.
- [12] K. Entacher, A. Uhl, and S. Wegenkittl. Linear and Inversive Pseudorandom Numbers for Parallel and Distributed Simulation. In *Twelfth Workshop on Parallel and Distributed Simulation PADS’98*, May 26th - 29th, 1998, pages 90–97, Banff, Alberta, Canada, 1998. IEEE Computer Society, Los Alamitos, California.
- [13] H. Leeb and S. Wegenkittl. Inversive and linear congruential pseudorandom number generators in empirical tests. *ACM Trans. Modeling and Computer Simulation*, **7**(2):272–286, 1997.

Refereed Proceedings and Contribution in Series

- [14] N. Benhabiles, P. Lackner, F.S. Domingues, S. Wegenkittl, A. Prlic, and M.J. Sippl. Assessing protein models: An evaluation of the performance of different score types. In H. D. Hötje and W. Sippl, editors, *Rational Approaches to Drug Design. Proceedings of the 13th European Symposium on Quantitative Structure-Activity Relationships. Aug 27 - Sep. 1, 2000*. Prous Science, Barcelona, Philadelphia.
- [15] S. Wegenkittl. Monkeys, gambling, and return times: Assessing pseudorandomness. In P.A. Farrington, H.B. Nembhard, D.T. Sturrock, and G.W. Evans, editors, *Proceedings of the 1999 Winter Simulation Conference*, pages 625–631. IEEE Press, 1999.
- [16] K. Entacher, A. Uhl, and S. Wegenkittl. Parallel random number generation: Long-range correlations among multiple processors. In P. Zinterhof, M. Vajteršic, and A. Uhl, editors, *Parallel Computation*, volume 1557 of *Lecture Notes in Computer Science*, pages 107–116. Springer, New York, 1999.
- [17] K. Entacher, A. Uhl, and S. Wegenkittl. Linear Congruential Generators for Parallel Monte-Carlo: the Leap-Frog Case. *Monte Carlo Methods and Appl.*, **4**(1):1–16, 1998.
- [18] J. Eichenauer-Herrmann, E. Herrmann, and S. Wegenkittl. A survey of quadratic and inversive congruential pseudorandom numbers. In H. Niederreiter, P. Hellekalek, G. Larcher, and P. Zinterhof, editors, *Monte Carlo and Quasi-Monte Carlo Methods 1996*, number 127 in *Lecture Notes in Statistics*, pages 66–97. Springer, New York, 1997.

Technical Reports

- [19] K. Entacher, B. Hechenleitner, and S. Wegenkittl. A simple OMNeT++ queuing experiment using parallel streams. In R. Trobec, P. Zinterhof, M. Vajteršic, and A. Uhl, editors, *Proceedings of the international workshop Parallel Numerics ’02*, 2002.

- [20] S. Wegenkittl. The pLAB picturebook: Load tests for the SG100 security generator. Report no. 8, pLAB – reports, University of Salzburg, 1998.
- [21] K. Entacher and S. Wegenkittl. Analyzing Streams of Pseudorandom Numbers for Parallel Monte Carlo Integration. In R. Wyrzykowski, H. Piech, M. Vajteršić, and P. Zinterhof, editors, *Proceedings of the international Workshop Parallel Numerics' 97*, pages 59–71, Zakopane, Poland, 1997.
- [22] S. Wegenkittl. The pLAB picturebook: Load tests and ultimate load tests, part I. Report no. 1, pLAB – reports, University of Salzburg, 1997.
- [23] K. Entacher and S. Wegenkittl. The pLAB picturebook: Load tests and ultimate load tests, part II: Subsequences. Report no. 2, pLAB – reports, University of Salzburg, 1997.
- [24] S. Wegenkittl and K. Entacher. On the relevance of splitting properties and the compound method in parallel applications of pseudorandom number generators. In R. Trobec, M. Vajteršić, P. Zinterhof, J. Šilc, and Robič B., editors, *Proceedings of the international workshop Parallel Numerics '96*. CEI-PACT Project, WP5.1.2.1.2, 1996.
- [25] P. Hellekalek, K. Entacher, S. Wegenkittl, and A. Weingartner. Extension of the tables of IMP-polynomials. Report D5H-5, CEI-PACT Project, WP5.1.2.1.2, Research Institute for Software Technology, University of Salzburg, Austria, 1995.
- [26] S. Wegenkittl. On empirical testing of pseudorandom number generators. In G. De Pietro, A. Giordano, M. Vajteršić, and P. Zinterhof, editors, *Proceedings of the international workshop Parallel Numerics '95*. CEI-PACT Project, WP5.1.2.1.2, 1995.

Articles in Popular Scientific Journals

- [27] S. Wegenkittl and R. Schistek. Qualitätsmanagement in der Koronarchirurgie. *NOEO Wissenschaftsmagazin Salzburger Bildungs- und Forschungseinrichtungen*, 3:18–20, 2004.
- [28] S. Wegenkittl. Von Zufall und Ähnlichkeit: Affenprosa, Glücksräder und Zufallstexte. *NOEO Wissenschaftsmagazin Salzburger Bildungs- und Forschungseinrichtungen*, 4:42–45, 2003.
- [29] S. Wegenkittl. Nicht Alles dem Zufall überlassen: Wie erkennen Handy und PDA ihre Stimme und Schrift? *NOEO Wissenschaftsmagazin Salzburger Bildungs- und Forschungseinrichtungen*, 4:46–49, 2003.

Invited Talks

- *Entropy based Tests for Randomness and Application to Cryptographic Generators*, June 17–28, 2002, Workshop on Random Number Generators and Highly Uniform Point Sets, CRM, Montreal, invited by Prof. L'Ecuyer.
- *Monkeys, Gambling, and Return Times: Assessing Pseudorandomness*, Dezember 5, 1999, Winter Simulation Conference, Phoenix, Arizona,
- *Memory Tests for Sparse Matrix Generators*, November 26, 1998, University of Economics and Business Administration, Department for Applied Statistics and Data Processing, invited by Prof. Derflinger.

- *Serielle Tests und Besuchshäufigkeiten in Markov Ketten*, Workshop Pseudozufallszahlen, October 15, 1998, Technische Hochschule Darmstadt, Germany, invited by Doz. Dr. Jürgen Eichenauer-Herrmann.
- *ϕ -Divergenzen: Eine Goodness-of-fit Klasse für sich.*, Offenes Seminar der AG 9, April 24, 1997, Technische Hochschule Darmstadt, Germany, invited by Doz. Dr. Jürgen Eichenauer-Herrmann.
- *Inversive Congruential Generators: the Results of an Exhaustive Series of Empirical Tests*, Workshop on pseudorandom number generation, June 3-21, 1996, Centre de recherches mathématiques, Université de Montréal, Canada, invited by Professor P. L'Ecuyer.
- *Über "statistische Qualitäten" pseudozufälliger Zahlen*, Workshop Pseudozufallszahlen, February 1996, Technische Hochschule Darmstadt, Germany, invited by Hr. Doz. Dr. Jürgen Eichenauer-Herrmann.

Talks

- *Entropy in parallel Streams of Pseudorandom Numbers*, International Workshop on Parallel Numerics, October 23-25, 2002, Bled, Slovenia.
- *Conditional Entropy Measures for Pseudorandom Numbers*, Third IMACS seminar on Monte Carlo methods, September 10-14, 2001, Salzburg, Austria.
- *Gambling Tests*, Second IMACS seminar on Monte Carlo methods, June 7-11, 1999, Varna, Bulgaria.
- *Parallel Random Number Generation: Long Range Correlations among Multiple Processors*, together with Karl Entacher (speaker) and Andreas Uhl, 4'th International Conference of the ACPC Feb. 16–18, 1999, Salzburg, Austria.
- *On pseudo-randomness: generators, applications, and tests*, Séminaire de Théorie des Nombres et Algorithmique, September 24, 1998, Université de Provence, France.
- *Structures in the Scatterplots of inversive generators*, Third International Conference on Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing, July 22–26, 1998, Claremont, California USA.
- *Hyperbelstrukturen bei explizit inversen Pseudozufallszahlengeneratoren*, 14. ÖMG Kongress, September 23, 1997, University of Salzburg, Austria.
- *On the Relevance of Splitting Properties and the Compound Method in Parallel Applications of Pseudorandom Number Generators*, International Workshop Parallel Numerics '96, September 11, 1996, Gozd Martuljek, Slovenia.
- *Extensive empirical testing of inversive and quadratic congruential generators*, Second International Conference on Monte Carlo and Quasi-Monte Carlo Methods in Scientific Computing, July 9–12, 1996, University of Salzburg, Austria.
- *Zum statistischen Testen von Zufallszahlengeneratoren*, Minisymposium "Pseudozufallszahlen und Quasi-Monte Carlo Methoden", Oktober 6, 1995, Technische Hochschule Darmstadt, Germany.

- *On Empirical Testing of Pseudorandom Number Generators*, International Workshop Parallel Numerics '95, September 27, 1995, Sorrento Palace Hotel, Italy.
- *Empirical Results with Marsaglia's Overlapping M-tuple test*, Minisymposium aus Mathematischer Statistik und Stochastiktag, March 23, 1995, Vienna, Austria.

Research Positions Abroad

- August 30 till September 12, 2004, Université d'Aix-Marseille I, Centre de Mathématiques et Informatique, France, invited by Prof. Pierre Liardet.
- September 21 till Oktober 2, 1998, Université d'Aix-Marseille I, Centre de Mathématiques et Informatique, France, invited by Prof. Pierre Liardet.
- April 22 till April 29, 1997, Technische Hochschule Darmstadt, invited joined research with Doz. Dr. Jürgen Eichenauer-Herrmann.
- February 23 till March 22, 1997, Université de Montréal, invited joined research with Prof. P. L'Ecuyer, Centre de recherches mathématiques on "Power divergence tests for Pseudorandom number generators, the overlapping case".
- November 27 till December 2, 1995, Technische Hochschule Darmstadt, invited joined research with Doz. Dr. Jürgen Eichenauer-Herrmann on "Strukturelle Eigenschaften inverser Generatoren (Hyperbelstrukturen)".