

Stephen Anthony Fenner

Office: Department of Computer Science and Engineering
University of South Carolina
Columbia, South Carolina 29208
(803) 777-2596
fenner@cse.sc.edu
<http://www.cse.sc.edu/~fenner>

Research Expertise and Interests

Quantum Computing and Information:

algorithms, complexity theory, communication protocols

Computational complexity theory:

relationships among complexity classes, structure of complexity classes, counting classes, resource-bounded reductions, resource-bounded measure and category, logic and descriptive complexity

Cryptology and Network Security:

cryptographic protocols and cryptanalysis, proofs of security, mobile code security, quantum cryptography

Programming languages and semantics

Physics of computation

Computability theory

Machine learning

Software engineering

Education

University of Chicago, Chicago, Illinois.

Ph.D. in Computer Science, June 1991.

Thesis Title: Chains, Gaps, and Finite Extensions: Three Topics in Structural Complexity.

Thesis Advisor: Stuart Kurtz.

M.S. in Computer Science, June 1988.

Harvard University, Cambridge, Massachusetts.

B.A. in Physics *cum laude*, June 1983.

Academic Positions

University of South Carolina, Columbia, South Carolina.

Associate Professor in Computer Science, August 1999–present.

University of South Carolina, Columbia, South Carolina.

Visiting Associate Professor in Computer Science, August 1998–May 1999.

University of Southern Maine, Portland, Maine.

Associate Professor in Computer Science, August 1997–July 1999.

Assistant Professor in Computer Science, August 1991–July 1997.

University of Chicago, Chicago, Illinois.

Lecturer in Computer Science, January 1986–December 1990.

Grants, Awards, and Grant Submissions

National Science Foundation. “Information Systems Security Education” (co-PI) with Csilla Farkas

(PI) and Caroline M. Eastman, Duncan A. Buell, and Joseph E. Johnson (co-PIs).
September 2001–August 2003. \$199,846. Accepted.

National Science Foundation. ITR/SY in “Algorithms in Quantum Computation and Communications” (sole PI). Submitted January 2001. Declined.

S. C. Commission on Higher Education. Research in “Algorithms in Quantum Computation and Communications” (sole PI). Submitted September 2000. January 2001–December 2001. \$30,000. Accepted.

S. C. Commission on Higher Education. Research in “Computer Systems to Detect Fraud and Illegal Activities” (PI) with Caroline Eastman and John Rose (co-PIs). Submitted September 1999. \$102,500 for one year. Declined.

University of South Carolina College of Science and Mathematics. Start-up funds. July 1999–June 2001. \$50,000.

National Science Foundation. CAREERS grant renewal CCR-9996310. July 1999–June 2000. \$16,000. Accepted.

National Security Agency. Research in “Limitations on Quantum Computation” (co-PI) with Lance Fortnow (PI) and John Rogers (PI). Submitted March 1999. Declined.

Office of Naval Research. Small business proposal in “Secured Voice over Wide-Area Networks” (consultant) with Bruce Buller. Submitted January 1999. Declined.

South Carolina EPSCoR. Grant preproposal to National Science Foundation in “Forensic Computing” (co-PI) with Caroline Eastman (PI) and John Rose (co-PI). Submitted October 1998. Declined.

National Science Foundation. CAREERS grant in “Properties of Typical Computable Languages” CCR-9501794 (PI). July 1995–June 1998. \$92,000.

USM School of Applied Science. First Faculty Award for Excellence in Scholarship, July 1997–June 1998. \$650.

International Conference and Research Center for Computer Science, Schloss Dagstuhl. Participated in invitational seminars on structural complexity theory, partially subsidized by the Center, in Wadern, Germany. February 13–18, 1994, and September 29–October 4, 1996. Subsidized food and lodging expenses.

National Science Foundation. Research Initiation Award in “Counting Classes and Resource-Bounded Measure and Category” CCR-9209833 (PI). July 1992–June 1995. \$60,000.

University of Chicago. University Fellowship. January 1991–June 1991.

Professional Activities and Memberships

Founder, host, and chief presenter, University of South Carolina Quantum Computing Seminar (an interdepartmental weekly seminar). January 2000–present.

Program committee member, 13th Annual IEEE Conference on Computational Complexity (formerly Structure in Complexity Theory), Buffalo, New York, June 1998.

Program committee member, 13th Annual GI/AFCET Symposium on Theoretical Aspects of Computer Science, Grenoble, France, February 1996.

Maine Workshop in Structural Complexity. Planned, organized, and conducted first three meetings of an invitational workshop in complexity theory at the Stone House, Wolfe’s Neck, Maine, August 21–24, 1993, August 6–10, 1995, and August 18–22, 1997. Each meeting had 12–23 colleagues and students from across the United States and Europe, and included talks, nature walks, reception and lobster bake.

Referee for *SIAM Journal on Computing*, *Theoretical Computer Science*, *Mathematical Systems Theory, Information and Computation*, *Journal of Symbolic Logic*, *Journal of Computer and System Sciences*, *Information Processing Letters*, Cambridge University Press, Addison-Wesley.

Subreferee for 15th Annual GI/AFCET Symposium on Theoretical Aspects of Computer Science, 1998; 9th Annual IEEE Structure in Complexity Theory conference, 1994.

Member, Association for Computing Machinery, SIGSAC, SIGPLAN, SIGACT, Association for Symbolic

Logic.

Administrative Service

University of South Carolina

Chair, Computer Science Department Colloquium Committee, August 1999–present.

Member, CS Department Undergraduate and Qualifying Exam Committees, August 1999–present.

University of Southern Maine

Departmental liaison to the Portland Office of Economic Development and the Maine Software Developers Association, September 1997–April 1998.

Made initial contacts and helped organize ongoing cooperation with local industry, including job fairs, industry seminars, and internship programs.

Chair, CS Department Curriculum Committee, September 1992–June 1994, September 1996–June 1998.

Developed new core course, Deductive Logic, especially designed for students in the Computer Science, Mathematics, and Philosophy departments, and for students in the USM Honors program.

Chair, USM Distinguished Faculty Award Committee, Spring 1992.

Selected a faculty member to receive annual award for excellence in teaching, research, academic and community service.

Chair, CS Department Colloquium Committee, Fall 1993–Spring 1996.

Member, CS Department Personnel, Library, and Faculty Search Committees.

Member, USM Presidential Scholarship Committee, Spring, 1995.

Selected outstanding USM students for academic scholarships.

Nonacademic Experience

L. L. Bean, Freeport Maine.

Web programming consultant, July–August 1997, April–May 1998 (part time), June–August 1998 (full time). Wrote web site/electronic commerce software to convert catalog text into HTML and organize product pages. Also wrote tools to summarize and analyze firewall-generated network traffic logs.

Passive Power Products, Gray, Maine.

Software consultant, June 1993–January 1995 (part time). Verified, enhanced, and debugged embedded, real-time transmitter/antenna monitoring software.

The University of Chicago Center for Information and Language Studies, Chicago, Illinois.

Programmer and analyst, June 1990–December 1990 (part time). Developed text processing software for the American and French Research on the Treasury of the French Language (ARTFL) text improvement and data compression project. Used UNIX shell scripts, awk, and lex.

Doblin, Keeley, Malin and Associates, Chicago, Illinois.

Programmer and analyst, June 1989–March 1990. Developed desk-top publishing software (including graphics user interface, intermediate page description language, and PostScript printer driver) in Smalltalk and C.

Computer Innovations, Inc., Chicago, Illinois.

Programmer and analyst, June 1987–December 1987. Wrote database and text processing software, software documentation.

Publications and Presentations

Stephen A. Fenner

Refereed Journals and Conferences

[These publications are available at <http://www.cs.sc.edu/~fenner/pubs.html>]

S. Fenner, S. Homer, M. Schaefer, R. Pruim. Hyper-polynomial hierarchies and the polynomial jump. *Theoretical Computer Science*. Volume 262 (2001), pages 241–256. Also appeared in *Proceedings of the 12th Annual IEEE Conference on Computational Complexity*, Ulm, Germany, June 1997, pages 102–110.

H. Buhrman, S. Fenner, L. Fortnow, L. Torenvliet. Two oracles that force a big crunch. To appear in *Computational Complexity*. Combination of two previous conference papers, including

S. Fenner, L. Fortnow. Beyond $\mathbf{P}^{\mathbf{NP}} = \mathbf{NEXP}$. *Proceedings of the 12th Annual GI/AF CET Symposium on Theoretical Aspects of Computer Science*, Munich, Germany, March 1995, pages 619–627.

H. Buhrman, S. Fenner, L. Fortnow, D. van Melkebeek. Optimal proof systems and sparse sets. *Proceedings of the 17th Annual GI/AF CET Symposium on Theoretical Aspects of Computer Science*, Lille, France, February 2000. Lecture Notes in Computer Science, volume 1770 (2000), Springer, Berlin, pages 407–418.

S. Fenner, F. Green, S. Homer, R. Pruim. Determining acceptance possibility for a quantum computation is hard for the polynomial hierarchy. *Proceedings of the Royal Society, London A* (1999). Volume 455, pages 3953–3966. E-print archive: quant-ph/9812056. Also appeared in *Proceedings of the Sixth Italian Conference on Theoretical Computer Science*, Tuscany, Italy, November 1998, pages 241–252.

S. Fenner, F. Green, S. Homer, A. Selman, T. Thierauf, H. Vollmer. Complements of many-valued functions. *Chicago Journal of Theoretical Computer Science*. Volume 1999(3) (1999). Also appeared in *Proceedings of the Eleventh Annual IEEE Conference on Computational Complexity*, Philadelphia, PA, May 1996, pages 260–269.

S. Fenner, M. Schaefer. A note on a variant of immunity, btt-reducibility, and minimal programs. *Mathematical Logic Quarterly*. Volume 45 (1999), pages 3–21.

S. Fenner, S. Homer, M. Ogihara, A. Selman. Oracles that compute values. *SIAM Journal on Computing*. Volume 26 (1997), pages 1043–1065. Also appeared in *Proceedings of the 10th Annual GI/AF CET Symposium on Theoretical Aspects of Computer Science*, Würzburg, Germany, February 1993, pages 398–407.

H. Buhrman, S. Fenner, and L. Fortnow. Results on resource-bounded measure. *Proceedings of the 24th International Colloquium on Automata, Languages and Programming*, Bologna, Italy, July 1997. Lecture Notes in Computer Science, volume 1256 (1997), Springer, pages 188–194.

S. Fenner, L. Fortnow, L. Li. Gap-definability as a closure property. *Information and Computation*. Volume 130 (1996), pages 1–17. Also appeared in *Proceedings of the Tenth Annual GI/AF CET Symposium on Theoretical Aspects of Computer Science*, Würzburg, Germany, February 1993, pages 484–493.

S. Fenner, L. Fortnow, A. Naik, J. Rogers. Inverting onto functions. *Proceedings of the Eleventh Annual IEEE Conference on Computational Complexity*, Philadelphia, PA, May 1996, pages 213–222.

S. Fenner, L. Fortnow, S. Kurtz. The isomorphism conjecture holds relative to an oracle. *SIAM Journal on Computing*. Volume 25 (1996), pages 193–206. Also appeared in *Proceedings of the 33rd Annual IEEE Symposium on Foundations of Computer Science*, Pittsburgh, PA, October 1992, pages 30–39.

S. Fenner, J. Lutz, E. Mayordomo. Weakly useful sequences. *Proceedings of the 22nd EATCS International Colloquium on Automata, Languages, and Programming*, Szeged, Hungary, July 1995. Lecture Notes in Computer Science, volume 944 (1995), Springer, pages 393–404.

S. Fenner. Inverting the Turing jump in complexity theory. *Proceedings of the Tenth Annual IEEE Conference on Structure in Complexity Theory*, Minneapolis, MN, June 1995, pages 102–110.

S. Fenner. Resource-bounded Baire category: A stronger approach. *Proceedings of the Tenth Annual IEEE Conference on Structure in Complexity Theory*, Minneapolis, MN, June 1995, pages 182–192.

- S. Fenner. Almost weakly 2-generic sets. *Journal of Symbolic Logic*. Volume 59 (1994), pages 868–887.
- S. Fenner, L. Fortnow, S. Kurtz, L. Li. An oracle builder's toolkit. *Proceedings of the Eighth Annual IEEE Conference on Structure in Complexity Theory*, San Diego, CA, May 1993, pages 120–131.
- S. Fenner, L. Fortnow, S. Kurtz. Gap-definable counting classes. *Journal of Computer and System Sciences*, special issue of best papers from the 1991 IEEE Conference on Structure in Complexity Theory. Volume 48 (1994), pp. 116–148. Also appeared in *Proceedings of the Sixth Annual IEEE Conference on Structure in Complexity Theory*, Chicago, IL, July 1991, pages 30–42.
- S. Fenner. Notions of resource-bounded category and genericity. *Proceedings of the Sixth Annual IEEE Conference on Structure in Complexity Theory*, Chicago, IL, July 1991, pages 196–212.
- S. Fenner, S. Kurtz, J. Royer. Every polynomial-time 1-degree collapses iff $P = PSPACE$. *Proceedings of the 30th Annual IEEE Symposium on Foundations of Computer Science*, Research Triangle Park, NC, October 1989, pages 624–29.

Manuscripts, Submissions, and Unrefereed Publications

- S. Fenner, S. Kurtz, J. Royer. Every polynomial-time 1-degree collapses iff $P = PSPACE$. Submitted to *Journal of Symbolic Logic* November 2000.
- S. Fenner. An intuitive Hamiltonian for quantum search. University of South Carolina Department of Computer Science and Engineering Technical Report CSE-TR-2000-1, April 2000. E-print archive: quant-ph/0004091. Submitted to FOCS 2000.
- S. Fenner, L. Fortnow, A. Naik, J. Rogers. Inverting onto functions. Submitted to *Information and Computation* May 1998.
- S. Fenner, M. Schaefer. Simplicity and Strong Reductions. Submitted to *Information and Computation* May 1998.
- S. Fenner, L. Fortnow, W. Gasarch. Complexity theory newsflash. *SIGACT News*. Volume 27(3), 1996, page 126.
- L. Barrett, S. Fenner. Second Maine Summer Workshop in Structural Complexity. *SIGACT News*. Volume 27(3), 1996, pages 119–120.
- M. Böttcher, S. Fenner. Some limits on resource-bounded diagonalizations in relativized complexity. Manuscript.
- L. Barrett, S. Fenner. First Maine Workshop in Structural Complexity. *SIGACT News*. Volume 25(1), 1994, pages 82–83.
- S. Fenner. Chains, Gaps, and Finite Extensions: Three Topics in Structural Complexity. Ph.D. thesis, University of Chicago, Chicago, IL, June 1991. Available as University of Chicago Department of Computer Science Technical Report 91–18.
- S. Fenner. Tight lower bounds on genericity required to prevent one-way functions. University of Chicago Technical Report 91–04, 1991.

Invited Presentations

- An Intuitive Hamiltonian for Quantum Search*. Thirty-first Winter Colloquium on the Physics of Quantum Electronics, Snowbird, Utah, January 8, 2001.
- Quantum versus Classical Computation: Power and Limitations*. University of South Carolina Mathematics Department Colloquium, Columbia, SC, February 29, 2000.
- Is BQP a counting class?* National Security Agency, Fort Meade, Maryland, January 25, 2000. Talk cancelled due to blizzard.
- Quantum Mechanics and Information Security*. University of South Carolina Physics Department Colloquium, Columbia, SC, October 14, 1999.
- Quantum Mechanics and Information Security*. University of South Carolina Mathematics Department Industrial Mathematics Institute Colloquium, Columbia, South Carolina, May 10, 1999.

An Exact Characterization of Quantum NP. National Security Agency, Fort Meade, Maryland, March 11, 1999.

An Exact Characterization of Quantum NP. Poster session, Second Workshop on Algorithms in Quantum Information Processing, Chicago, IL, January 18–22, 1999.

Counting Complexity and Quantum Computation (survey). University of Maine Computer Science Department Seminar, Orono, ME, October 6, 1997.

Inverting Onto Functions. Invited talk at 906th Meeting of the American Mathematical Society, special session on Complexity Theory, Greensboro, NC, November 17, 1995.

Resource-Bounded Baire Category: A Stronger Approach. Workshop on Complexity Theory, Institut für Informatik, Universität Ulm, Ulm, Germany, February 24, 1995.

Resource-Bounded Baire Category: A Stronger Approach. Institut für Informatik, Universität Lübeck, Lübeck, Germany, February 22, 1995.

Resource-Bounded Baire Category: A Stronger Approach. Midwest Theory Day, University of Chicago, December 3, 1994.

On Inverting the Turing Jump in Complexity Theory. International Conference and Research Center for Computer Science, Schloss Dagstuhl, invitational Seminar in Structural Complexity, Dagstuhl, Germany. February 17, 1994.

Conference Presentations

Complements of Multivalued Functions. Eleventh Annual IEEE Conference on Computational Complexity, Philadelphia, PA, May 24, 1996.

Inverting the Turing Jump in Complexity Theory. Tenth Annual IEEE Conference on Structure in Complexity Theory, Minneapolis, MN, June 29, 1995.

Resource-Bounded Baire Category: A Stronger Approach. Tenth Annual IEEE Conference on Structure in Complexity Theory, Minneapolis, MN, June 30, 1995.

Beyond $P^{NP} = NEXP$. GI/AFCEC Symposium on Theoretical Aspects of Computer Science, München, Germany, March 4, 1995.

Gap-Definability as a Closure Property. GI/AFCEC Symposium on Theoretical Aspects of Computer Science, Würzburg, Germany, February 26, 1993.

Notions of Resource-Bounded Category and Genericity. Sixth Annual IEEE Conference on Structure in Complexity Theory, Chicago, IL, July 2, 1991.

Every Polynomial-Time 1-Degree Collapses iff $P = PSPACE$. 30th Annual IEEE Symposium on Foundations of Computer Science, Research Triangle Park, NC, November 1, 1989.

Other Presentations

Quantum Computation and Communication. Seminar sponsored by the American Society of Mechanical Engineers, Central Savannah River Area Section, Aiken, SC (USC campus), March 24, 2001.

Internet and Computer Security. Seminar sponsored by the American Society of Mechanical Engineers, Central Savannah River Area Section, Aiken, SC (USC campus), October 30, 1999.

Forensic Computing. University of South Carolina College of Science and Mathematics, University 101 Explorer's Night, Columbia, SC, October 26, 1999.

Factoring on a Quantum Computer (work of Shor). Summus Ltd. weekly meeting. July 24, 31, 1999.

Quantum Mechanics and Information Security. University of South Carolina Computer Science Colloquium, Columbia, SC, February 18, 1999.

Counting Complexity, GapP, and Quantum Computation. University of Chicago Computer Science Seminar, Chicago, IL, February 18, 1998.

Counting Complexity (survey). DePaul University Computer Science, Telecommunications, and Information Systems Seminar, Chicago, IL, February 17, 1998.

An Introduction to Quantum Computation (survey). University of Southern Maine Mathematics Seminar, Portland, ME, December 4, 1997.

A Hard Problem in Quantum Computation. Boston University Complexity Theory Seminar, Boston, MA, October 24, 1997.

A New Oracle for the Isomorphism Conjecture (work of Beigel, Buhrman, and Fortnow). Boston University Complexity Theory Seminar, Boston, MA, April 25, 1997.

A Descriptive Complexity Approach to Graph Canonization (work of Cai, Furst, and Immerman). Boston University Complexity Theory Seminar, Boston, MA, April 19, 1996.

Proving Nonexpressibility in Finite Models with Ehrenfeucht-Fraïssé Games (survey). Boston University Complexity Theory Seminar, Boston, MA, April 12, 1996.

Inverting Onto Functions. Boston University Complexity Theory Seminar, Boston, MA, November 24, 1995.

Towards a Transfinite Polynomial Hierarchy. Boston University Complexity Theory Seminar, Boston, MA, February 10, 1995.

Quantum Cryptography (work of Brassard, et al.). University of Southern Maine Computer Science Department Colloquium, December 9, 1994.

Towards a Transfinite Polynomial Hierarchy. University of Chicago Computer Science Department Theory Colloquium, December 2, 1994.

Factoring on a Quantum Computer (work of Peter Shor). Boston University Complexity Theory Seminar, Boston, MA, October 24, 1994.

Complete Sets for $NP \cap SPARSE$. Joint Northeastern University/Boston University Complexity Theory Seminar, Boston, MA, March 11, 1994.

Computing Single-Valued Refinements of Total NP Functions. Joint Northeastern University/Boston University Complexity Theory Seminar, Boston, MA, October 15, 1993.

Logical Characterizations of Complexity Classes (work of Papadimitriou and Yanakakis). Joint Northeastern University/Boston University Complexity Theory Seminar, Boston, MA, April 30, 1993.

On the Nonuniform Complexity of the Graph Isomorphism Problem (work of Lozano and Torán). Joint Northeastern University/Boston University Complexity Theory Seminar, Boston, MA, December 11, 1992.

The Isomorphism Conjecture Holds Relative to an Oracle. IEEE Conference on Structure in Complexity Theory, Boston, MA, June 22, 1992. Rump session.

The Isomorphism Conjecture Holds Relative to an Oracle. Joint Northeastern University/Boston University Complexity Theory Seminar, Boston, MA, June 5 and 12, 1992.

Generic Oracles in Complexity Theory. Joint Northeastern University/Boston University Complexity Theory Seminar, Boston, MA, March 20 and 27, 1992.

Gap-Definable Counting Classes. Joint Northeastern University/Boston University Complexity Theory Seminar, Boston, MA, October 25, 1991.

Teaching and Advising

Stephen A. Fenner

Subjects

Direct experience teaching the following subjects:

Undergraduate

- Advanced Calculus
- Algorithms and data structures in Pascal, C++
- Assembly language programming
- Compiler design and construction
- Data structures in C
- Deductive logic (propositional and predicate calculus)
- Functional programming in Scheme
- Introduction to databases
- Introductory programming in Pascal, C++
- Introductory programming in Scheme (honors)
- Programming languages
- Theory of computation (automata, languages, Turing machines)

Graduate

- Advanced theory of computation (computability, complexity)
- Cryptography
- Network Security

Background and interest to teach courses in the following additional areas:

- Abstract algebra
- Advanced algorithm design and analysis
- Advanced data structures
- Calculus
- Computational complexity theory
- Computer graphics
- Differential Geometry
- Discrete mathematics
- Mathematical logic
- Number theory
- Recursive function theory
- Set theory
- Software engineering
- Topology

Institutions

University of South Carolina, Columbia, South Carolina, August 1998–present.

Courses developed and taught:

Computer Networks (Network Security, graduate).

Cryptographic protocols, confidential communication, hashes, digital signatures, authentication protocols, key distribution, secure electronic mail, cryptanalytic and other attacks.

Text: Kaufman, Perlman, Speciner, *Network Security: Private Communication in a Public World*.

Cryptography (graduate).

Information theory, secret-key cryptography, block ciphers, DES, cryptanalysis, public-key cryptography, number-theory, RSA, Diffie-Hellman, ElGamal, secret-sharing, elliptic curve and lattice reduction-based cryptography.

Texts: Stinson, *Cryptography: Theory and Practice* and Schneier, *Applied Cryptography*.

Course taught:

Introduction to Algorithmic Design I (C++).

First-semester programming.

Text: Savitch, *Problem Solving with C++: The Object of Programming (2nd ed.)*.

Programming Languages.

Programming language design and implementation techniques used in several different programming paradigms, student implementation of a Scheme interpreter.

Text: Sethi, *Programming Languages: Concepts and Constructs (2nd ed.)*.

University of Southern Maine, Portland, Maine, August 1991–present.

Courses developed and taught:

Deductive Logic.

Translating English into symbolic logical notation, truth-functional logic, truth tables, predicate logic and quantifiers, rules for transforming truth-functional and quantified formulae, a system of formal deduction.

Text: Goldfarb, *Deductive Logic* (course notes).

Functional Programming in Scheme.

Programming in the functional language Scheme (a dialect of Lisp). Techniques for designing large, flexible systems, including generic arithmetic packages, symbolic computation systems, and circuit simulators. Additionally the λ -calculus is studied as a formal precursor to Scheme.

Text: Abelson & Sussman, *Structure and Interpretation of Computer Programs*.

Advanced Theory of Computation (graduate).

Computability theory, computable functions, computable and computably enumerable sets, Gödel's incompleteness theorem, Turing machines, resource bounded computation, relativized computation, reductions, NP-completeness, complexity theoretic hierarchies.

Courses taught:

Introduction to Compiler Construction.

Lex and yacc, theory of parsing and syntax-directed translation, type checking, and code generation and optimization. Students complete the bulk of a working C compiler.

Text: Aho, Sethi, & Ullman, *Compilers: Principles, Techniques, and Tools*.

Programming Languages.

Design and implementation issues, including imperative, functional, and logic programming, type inference, parametric polymorphism, and object-oriented systems. Students implement a Scheme interpreter.

Languages studied: Pascal, Modula-2, C, C++, Scheme, ML, and Prolog.

Text: Sethi, *Programming Languages*.

Data Structures.

Intermediate topics in Data Structures, including linked lists, trees, hash tables, graphs, files. Applications to memory management, data bases, sorting, graph algorithms. Complexity analysis.

Text: Horowitz, Sahni, & Anderson-Freed, *Fundamentals of Data Structures in C*.

Structured Problem Solving: Pascal.

Text: Leestma & Nyhoff, *Turbo Pascal: Programming and Problem Solving*.

Algorithms in Programming (Pascal, C++).

Texts: Nyhoff & Leestma, *Data Structures and Program Design in Pascal*, 2nd ed; Adams, Leestma, & Nyhoff, *Turbo C++: An Introduction to Computing*; Deitel & Deitel, *C++ How to Program*.

University of Chicago, Chicago, Illinois.

Courses taught:

Introduction to Programming in Pascal I and II.

Introduction to Programming in Scheme I (honors).

Courses assisted:

Introduction to Programming in Pascal I.

Introduction to Programming in Scheme II (honors).

Theory of Computability.

The Johns Hopkins University Center for Academically Talented Youth, Lancaster, Pennsylvania.

Instructor in Precalculus, Summer 1988.

Harvard University Extension, Cambridge, Massachusetts.

Teaching Assistant and Section Leader, September 1984–June 1985.

Programming and Data Structures in VAX Assembly.

Multivariate Calculus.

Students Advised

Doctorate

Andrei Stoica. Research in quantum computing and information.

Masters

University of South Carolina

Thesis advisor,

Mayank Tiwari. “Integrating Separation of Duty Constraints and Role Templates in Role-Based Access Control.” July 2001.

Mehmet Agirtmis. “A Certificate Authority and Digital Signature Utility.” July 2001.

Ying Shen. “A Firewall for Windows 95/98 Personal Computers.” March 2001.

Kaleem Baig. “Web-Based Utilities for Cleaning Registry and Checking Installation in Windows 95/NT.” August 2000.

Thesis committee member,

V. Gopalan Sundaram. “A Small Image-Processing Program for the Microsoft Windows Environment.” July 2001.

Yang Li. “The design and implementation of on-line homework and tests.” May 2000.

Ramesh V. Nadimpalli. “Comparison of web interface for a tuberculosis diagnosis tool using CGI and servlets.” December 1999.

Nagaraju Madiraju. “Multi-platform file explorer.” December 1999.

Kalyan Chakravarthy Paladugu. “A case study comparing web based application development technologies: Active server pages and Java (JDBC).” December 1999.

Rajan Kamatchi. “A simple editor for XML.” August 1999.

Yuqing Sun. “The authorization of web documents.” April 1999.

Crystal Fortner. “Survey of computer literacy knowledge among undergraduate students in computing.” April 1999.

Hongxin Chen. “The implementation of a Java multi-database interface.” December 1998.

Qing Yao, Kiran Mishra, Yong Zhang (ongoing).

University of Southern Maine

Xiangdong Sun. “Public key cryptography and RSA.” August 1998.

Marcus Schaefer. “A short history of minimal indices” (Computer Science Department, University of Chicago). December 1997.

Stephen Majercik. “Structurally dynamic cellular automata.” June 1994.

Martin Böttcher. “Genericity in complexity theory” (Universität Mainz, Abteilung für

Informatik). January 1996.

Matthew Levy.

Thesis committee member,

Margorie Harrison. "A Java applet for exploring graph problems." March 1998.

Stephen Dorato. "A fully bidirectional debugger." December 1995.

Leslie Pendleton, Matthew Levy, Sotero Giftos, Richard Best.