

Robert H. Gilman

Curriculum Vitae, December 2018

Education

A.B., Princeton University, June 1964

Ph.D., Columbia University, January 1969; Advisor: P. X. Gallagher

Contact

Department of Mathematical Sciences, Stevens Institute of Technology, Hoboken, NJ 07030

Tel: 201-216-5440

Email: rgilman@stevens.edu **Employment**

1982 - present	Professor	Stevens Institute of Technology
2003 Winter	Visitor	Imperial College
1999 - 2000	Visitor	City College of New York
1986 Winter	Visiting Professor	University of California at Santa Cruz
1982 - 1983	Visiting Professor	Rutgers University
1974 - 1982	Associate Professor	Stevens Institute of Technology
1969 - 1974	Assistant Professor	Stevens Institute of Technology

Honors and Awards

2016 Fall	Research Member	Mathematical Sciences Research Institute
2003 & 2014	Lecture Program	London Mathematical Society
1996 Spring	Research Professor	Mathematical Sciences Research Institute
1995 Fall	Visitor	Institut des Hautes Études Scientifiques
1991 - 1992	Member	Institute for Advanced Study
1984 - 1985	Member	Institute for Advanced Study
1971 - 1972	Postdoctoral Fellow	Courant Institute, New York University

Research Overview

Geometric group theory including applications of formal languages; classification of finite simple groups; also model theory, ergodic theory, complexity theory, and cryptology.

Doctoral Students

1. Yi-Di Zhang, Groups and ordinals by automata (2014); 2. Chih-Huei Wang, The generic free basis property (2011); 3. Parisa Babaali, Generic and structural properties of random regular languages (2007); 4. Hong Ray Cho, An introduction to counter groups (2006); 5. Li-Tien Wang, Evolutionary computation in coset enumeration (2001); 6. Mark Nichols, Quasi-realtime limited word replacement languages (1998); 7. Kathleen Kingston, Bianchi groups of class number one, (1993); 8. Scott Kolodziecki, δ -pseudo orbit shadowing in a family of trapezoidal maps (1991); 9. Harold Kruse, Groups whose characters satisfy an identity (1985); Sin-Min Lee, Investigations of simple universal algebras (1984).

Invited Lectures Since 2010

1. Searching for permutation groups, Manhattan Algebra Day, City University of New York, December 7, 2018 (scheduled).
2. Algorithmic randomness in group theory, North British Geometric Group Theory Seminar, Newcastle University, October 31, 2018.
3. Searching for random permutation groups, Hausdorff Institute of Mathematics, October 18, 2018

4. Generating the symmetric group, Mathematics Colloquium, Warwick University, October 12, 2018.
5. Algorithmic genericity in finitely presented Groups, Algebra Seminar, Warwick University, October 11, 2018.
6. Algorithmic genericity, New York Group Theory Seminar, February 9, 2018
7. The generic complexity of coset enumeration, Amer. Math. Soc. Special Session on Computational and Algorithmic Group Theory, Hunter College, CUNY, May 2017.
8. Algorithmic genericity, Group Theory Seminar, City University of New York, April 2017.
9. The complexity of coset enumeration, Workshop on Computation in Geometric and Combinatorial Group Theory, Edinburgh, July 2016.
10. The word problem for Z^2 , Equations and Formal Languages in Algebra, Les Diablerets, March 2016.
11. Public key cryptology and group theory, Hunter College Faculty Research Seminar, October 2015.
12. How to sample hard instances of the word problem, Group Theory Seminar, City University of New York, October 2015.
13. How useful is the word problem, Deutsche Mathematiker Vereinigung, Hamburg September 2015.
14. A partial algorithm for verifying automaticity, ALFA'15 (Automata, Logic, Formal languages and Algebra), Bordeaux, June 2015.
15. Universal groups of prees, Cornell Topology Festival, Ithaca, May 2015.
16. Variations on the word problem, Infinite Group Theory from the Past to the Future, Fairfield University and City University of New York, April 2015.
17. Triangles of prees, Group Theory Seminar, City University of New York, February 2015
18. Formal languages and group theory: beyond the Chomsky hierarchy, Algebra-Geometry Seminar, Newcastle, June 2014.
19. Small cancellation theory and hyperbolic groups, Algebra Seminar, St Andrews, June 2014.
20. Progress on the Andrews Curtis conjecture, Algebra Seminar, Warwick, May 2014.
21. Groups and complexity, Geometry of Computation in Groups, Schrödinger Institute, Vienna, April 2014.
22. Groups and circuits, Mathematical Problems of Informatics, Omsk, September, 2013.
23. New applications of formal language theory to group theory, Questions, Algorithms, and Computations in Abstract Group Theory Technische Universität Braunschweig, May 2013.
24. Automatic groups redux, Geometric and Asymptotic Group Theory with Applications, City College of New York, May, 2013
25. Generic properties of finitely presented groups, American Mathematical Society Special Session on Groups, Algorithms, Complexity, and Theory of Security, Boston, January 4, 2012.
26. Rational subsets of groups, Institute for Mathematical Sciences Workshop on Automata Theory and Applications, National University of Singapore, September 12, 2011.
27. Word hyperbolic groups, Lafayette-Lehigh Geometry-Topology Seminar, Lafayette College, March 26, 2011
28. Algorithmic Group Theory (2 talks), Workshop on Complexity and Group-based Cryptography, Centre de recherches mathématiques, Université de Montréal, August 30-31, 2010
29. Cryptology of infinite groups, Fourth Pythagorean Conference, Corfu, May 30–June 4, 2010.

30. The generic word problem, Amer. Math. Soc. Special Session on Logic and Groups, Newark, NJ, May 22–23, 2010.
31. Complexity of computations on compressed words, Amer. Math. Soc. Special Session on Groups, Computations, and Applications, Newark, NJ, May 22–23, 2010.
32. Postquantum cryptology for group theorists, Group Theory Seminar, City University of New York, March 12, 2010.
33. Group-theoretic cryptology, Algebra Seminar, City University of New York, March 5, 2010.

Refereed Publications

1. Groups whose word problems are not semilinear, *Groups, Complexity, Cryptology*, 10 (2018), 53–62 (with Saul Schleimer and Robert Kropholler).
2. Generalized small cancellation presentations for automatic groups, *Groups, Complexity, Cryptology*, 6 (2014), 93–101.
3. Random equations in nilpotent groups, *J. Algebra*, 352 (2012), 192–214 (with A. G. Miasnikov and V. Roman'kov).
4. Random equations in free groups, *Groups Complex. Cryptol.* 3 (2011), 257–284 (with A. G. Miasnikov and V. Roman'kov)
5. Exponentially generic subsets of groups, *Illinois J. Math.*, 54 (2010), 371–388 (with A. G. Miasnikov and D. Osin).
6. A geometric zero-one law, *J. Symbolic Logic* 74 (2009), 929–938 (with Y. Gurevich and A. G. Miasnikov).
7. Solving one-variable equations in free groups. *J. Group Theory* 12 (2009), 317–330 (with D. Bormotov and A. G. Myasnikov).
8. New developments in commutator key exchange, *Proc. First Int. Conf. on Symbolic Computation and Cryptography (SCC-2008)*, Beijing, 2008 (with A. G. Miasnikov, A. D. Myasnikov, and A. Ushakov).
9. A characterisation of virtually free groups, *Archiv der Mathematik*, **89**, 2007, 289–295 (with S. Hermiller, D. Holt, S. Rees).
10. Automatic quotients of free groups, *J. Pure Appl. Algebra*, **202**, 2005, 313–324.
11. Formal Languages and their Application to Combinatorial Group Theory, in *Groups, Languages, Algorithms*, Contemporary Mathematics, **378**, Amer. Math. Soc., 2005, 1–36.
12. One variable equations in free groups via context free languages. Computational and experimental group theory, 83-88, *Contemp. Math.*, **349**, Amer. Math. Soc., 2004 (with Alexei G. Myasnikov).
13. Word hyperbolic semigroups, *Math. Proc. Cambr. Phil. Soc.* **136**, 2004, 513-524 (with Andrew Duncan).
14. On the definition of word hyperbolic groups, *Mathematische Zeitschrift*, **242**, (2002) 529-541.
15. Context-free languages of sub-exponential growth, *Journal for Computer and System Sciences*, **64** (2002), 308–310 (with Martin Bridson).
16. Combing nilpotent and polycyclic groups, *Int. J. Algebra and Computation*, **9**, 1999, 135–155 (with Derek Holt and Sarah Rees).
17. Formal language theory and the geometry of 3-manifolds, *Commentarii Math. Helv.*, **71**, 1996, 525-555 (with Martin Bridson).
18. A shrinking lemma for indexed languages, *Theoretical Computer Sci.* **163**, 1996, 277-281.

19. Formal languages and infinite groups, in *Geometric and Computational Perspectives on Infinite Groups*, (Minneapolis, MN and New Brunswick, NJ, 1994), 27-51, DIMACS Ser. Discrete Math. Theoret. Comput. Sci., 25, Amer. Math. Soc., Providence, RI, 1996.
20. Automatic groups and string rewriting, in Proc. of the Ecole de Printemps d'Informatique Théorique, Font Romeu, May 17-21, 1993, Springer Lecture Notes in Comp. Sci. 1995
21. On bounded languages and the geometry of nilpotent groups, in *Combinatorial and Geometric Group Theory, Edinburgh 1993*, London Math. Soc. Lecture Notes **204**, Cambr. U. P. 1995, 1-15 (with Martin Bridson).
22. The geometry of cycles in the Cayley diagram of a group, in *The Mathematical Legacy of Wilhelm Magnus*, Contemporary Mathematics **169**, Amer. Math. Soc. 1994, 331-340.
23. A remark about combings of groups, Int. J. of Algebra and Computation **3**, 1993, 575-581 (with Martin Bridson).
24. Verifying that a group is virtually free, Int. J. Algebra and Computation **1** 1991, 339-351.
25. Periodic behavior of linear automata, in *Dynamical Systems*, J. C. Alexander ed., Lecture Notes in Mathematics **1349**, Springer Verlag 1988, 216-219.
26. Classes of linear automata, Ergodic Theory and Dyn. Sys. **7** 105-118, 1987.
27. Groups with a rational cross-section, in *Combinatorial Group Theory and Topology*, S. M. Gersten and J. R. Stallings eds., Princeton U. P. 1987
28. On the existence of cyclic surface kernels for pairs, J. London Math. Soc. **30** 451-464, 1985 (with J. Gilman).
29. Enumerating infinitely many cosets, in *Computational Group Theory*, M. Atkinson ed., Acad. Pr. 1984, 51-55.
30. An application of ultraproducts to finite groups, in *Proc. Rutgers Group Theory Year*, M. Aschbacher et. al. eds., Cambridge U. P. 1984, 409-412.
31. Computations with rational subsets of confluent groups, in *Eurosam '84 Proceedings*, Lecture Notes in Computer Science **174** , Springer Verlag 1984, 207-212.
32. Characteristically simple \aleph_0 -categorical groups, J. Symb. Logic **49** 1984, 900-907.
33. Finite groups with standard components of Lie type over fields of characteristic 2, J. Alg. **80** 1983, 383-516 (with R. Griess).
34. Enumeration of double cosets, J. Pure and Appl. Alg. **26** 1982, 183-188.
35. Odd standard components, Proc. Symp. Pure Math. **37** 1980, 85-90.
36. Presentations of groups and monoids, J. Alg. **57** 1979, 544-554.
37. Finite groups with small unbalancing 2-components, Pacific J. Math. **83** 1979, 55-106 (with R. Solomon).
38. Finite quotients of the automorphism group of a free group, Can. J. Math. **XXIX** 1977, 541-551.
39. Components of finite groups, Comm. in Alg. **4** 1976, 1133-1198.
40. Finite groups with Sylow 2-subgroups of class two I, Trans. Amer. Math. Soc. **207** 1975, 1-101 (with D. Gorenstein).
41. Finite groups with Sylow 2-subgroups of class two II, Trans. Amer. Math. Soc. **209** 1975, 103-126 (with D. Gorenstein).
42. A combinatorial identity with applications to representation theory, Illinois J. Math. **17** 1972, 347-351.
43. Complements to solvable Hall subgroups, Proc. Amer. Math. Soc. **27** 1971, 241-243.

Books

1. *Combinatorial and Geometric Group Theory*. Sean Cleary, Robert Gilman, Alexei G. Myasnikov and Vladimir Shpilrain eds., Contemporary Mathematics, 296. American Mathematical Society, 2002.
2. *Computational and Statistical Group Theory*. Robert Gilman, Alexei G. Myasnikov and Vladimir Shpilrain eds., Contemporary Mathematics, 298. American Mathematical Society, 2002.
3. *Groups, Languages and Geometry*. Robert Gilman, ed., Contemporary Mathematics, 250. American Mathematical Society, 1999.
4. *Geometric and Computational Perspectives on Infinite Groups*. Gilbert Baumslag, David Epstein, Robert Gilman, Hamish Short and Charles Sims, eds., DIMACS Series in Discrete Mathematics and Theoretical Computer Science, 25. American Mathematical Society, 1996.

Recent Service

1. *Administrative Positions at Stevens Institute of Technology*. Chair of Faculty Senate, 2013-2014. Director of the Algebraic Cryptography Center, 2009 - present. Director of the Department of Mathematical Sciences, 2004 - 2009 and 1997 - 2000. Associate Dean of the School of Sciences and Arts, 2000 - 2004.
2. *Editorial boards*. Groups, Complexity, Cryptology (de Gruyter) 2009 - present. Journal of Mathematical Cryptology (de Gruyter) 2008 - 2018. Algorithms and Computation in Mathematics, (Springer Verlag) 2003-2005, founding member.
3. *American Mathematical Society activities*. Eastern Section Program Committee, 2007-2009, Chair 2008-2009. Chair of organizing committees for AMS sectional meetings at Stevens Institute of Technology 2007 and 2001. Organizer of special sessions at AMS meetings 2007, 2005, and 2002.
4. *Other organizing committees chaired*. DIMACS Working Group and Tutorial on Exotic Constructions in Group Theory, Rutgers University, 2010. Workshop on Generic Complexity, American Institute of Mathematics, Palo Alto, 2007. Workshops on Computational Aspects of Geometric Group Theory at the Geometry Center and DIMACS, 1994.
5. *External review committees*: Queens College, CUNY (2017). Fairfield University (2014). Hunter College, CUNY (2012).
6. *Pedagogy*: Department committee to reform Stevens' calculus sequence, 2012-2015. Subsequent outcomes include a startup to develop novel educational software (<http://www.gradarius.com>).