

# Robert H. Gilman

## Curriculum Vitae

March, 2010

### Education

A.B.	Princeton University	June 1964
M.A.	Columbia University	June 1965
Ph.D.	Columbia University	January 1969
M.E. (H.C.)	Stevens Institute of Technology	June 1987

### Address

Department of Mathematics  
Stevens Institute of Technology  
Hoboken, NJ 07030  
Phone: 201.216.5440  
Email: rgilman@stevens.edu

### Employment

#### *Research Positions*

1982 - present	Professor	Stevens Institute of Technology
2003 Winter	Visitor	Imperial College
1999 - 2000	Visitor	City College of New York
1996 Spring	Research Professor	Mathematical Sciences Research Institute
1995 Fall	Visitor	Institut des Hautes Études Scientifiques
1991 - 1992	Member	Institute for Advanced Study
1986 Winter	Visiting Professor	University of California at Santa Cruz
1984 - 1985	Member	Institute for Advanced Study
1982 - 1983	Visiting Professor	Rutgers University
1974 - 1982	Associate Professor	Stevens Institute of Technology
1971 - 1972	Visiting Member	Courant Institute
1969 - 1974	Assistant Professor	Stevens Institute of Technology

#### *Administrative Positions at Stevens Institute of Technology*

2009 - present	Director	Algebraic Cryptography Center
2004 - 2009	Director	Department of Mathematical Sciences
2000 - 2004	Associate Dean	School of Sciences and Arts
1997 - 2000	Director	Department of Mathematical Sciences

### Doctoral Students

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

### Refereed Publications

1. A geometric zero-one law, *J. Symbolic Logic* 74 (2009), 929–938 (with Y. Gurevich and A. G. Miasnikov).
2. Solving one-variable equations in free groups. *J. Group Theory* 12 (2009), 317–330 (with D. Bormotov and A. G. Myasnikov).
3. 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).
4. A characterisation of virtually free groups, *Archiv der Mathematik*, **89**, 2007, 289–295 (with S. Hermiller, D. Holt, S. Rees).
5. Automatic quotients of free groups, *J. Pure Appl. Algebra*, **202**, 2005, 313–324.
6. Formal Languages and their Application to Combinatorial Group Theory, in *Groups, Languages, Algorithms*, *Contemporary Mathematics*, **378**, Amer. Math. Soc., 2005, 1–36.
7. 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).
8. Word hyperbolic semigroups, *Math. Proc. Camb. Phil. Soc.* **136**, 2004, 513–524 (with Andrew Duncan).
9. On the definition of word hyperbolic groups, *Mathematische Zeitschrift*, **242**, (2002) 529–541.
10. Context-free languages of sub-exponential growth, *Journal for Computer and System Sciences*, **64** (2002), 308–310 (with Martin Bridson).
11. Combing nilpotent and polycyclic groups, *Int. J. Algebra and Computation*, **9**, 1999, 135–155 (with Derek Holt and Sarah Rees).

12. Formal language theory and the geometry of 3-manifolds, *Commentarii Math. Helv.*, **71**, 1996, 525-555 (with Martin Bridson).
13. A shrinking lemma for indexed languages, *Theoretical Computer Sci.* **163**, 1996, 277-281.
14. 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.
15. 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
16. 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).
17. 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.
18. A remark about combings of groups, *Int. J. of Algebra and Computation* **3**, 1993, 575-581 (with Martin Bridson).
19. Verifying that a group is virtually free, *Int. J. Algebra and Computation* **1** 1991, 339-351.
20. Periodic behavior of linear automata, in *Dynamical Systems*, J. C. Alexander ed., Lecture Notes in Mathematics **1349**, Springer Verlag 1988, 216-219.
21. Classes of linear automata, *Ergodic Theory and Dyn. Sys.* **7** 105-118, 1987.
22. Groups with a rational cross-section, in *Combinatorial Group Theory and Topology*, S. M. Gersten and J. R. Stallings eds., Princeton U. P. 1987
23. On the existence of cyclic surface kernels for pairs, *J. London Math. Soc.* **30** 451-464, 1985 (with J. Gilman).
24. Enumerating infinitely many cosets, in *Computational Group Theory*, M. Atkinson ed., Acad. Pr. 1984, 51-55.
25. An application of ultraproducts to finite groups, in *Proc. Rutgers Group Theory Year*, M. Aschbacher et. al. eds., Cambridge U. P. 1984, 409-412.
26. Computations with rational subsets of confluent groups, in *Eurosam '84 Proceedings*, Lecture Notes in Computer Science **174**, Springer Verlag 1984, 207-212.
27. Characteristically simple  $\aleph_0$ -categorical groups, *J. Symb. Logic* **49** 1984, 900-907.
28. Finite groups with standard components of Lie type over fields of characteristic 2, *J. Alg.* **80** 1983, 383-516 (with R. Griess).
29. Enumeration of double cosets, *J. Pure and Appl. Alg.* **26** 1982, 183-188.

30. Odd standard components, Proc. Symp. Pure Math. **37** 1980, 85-90.
31. Presentations of groups and monoids, J. Alg. **57** 1979, 544-554.
32. Finite groups with small unbalancing 2-components, Pacific J. Math. **83** 1979, 55-106 (with R. Solomon).
33. Finite quotients of the automorphism group of a free group, Can. J. Math. **XXIX** 1977, 541-551.
34. Components of finite groups, Comm. in Alg. **4** 1976, 1133-1198.
35. Finite groups with Sylow 2-subgroups of class two I, Trans. Amer. Math. Soc. **207** 1975, 1-101 (with D. Gorenstein).
36. Finite groups with Sylow 2-subgroups of class two II, Trans. Amer. Math. Soc. **209** 1975, 103-126 (with D. Gorenstein).
37. A combinatorial identity with applications to representation theory, Illinois J. Math. **17** 1972, 347-351.
38. Complements to solvable Hall subgroups, Proc. Amer. Math. Soc. **27** 1971, 241-243.

#### Invited Publication

1. Report on generic case complexity, Herald of Omsk University, Special Issue, 2007, 103-110 (with A. G. Miasnikov, A. D. Myasnikov, and A. Ushakov).

#### Technical Report

1. A Geometric Zero-One Law, Microsoft Research Technical Report MSR-TR-2007-63, June 2007 (with Y. Gurevich and A. G. Miasnikov)

#### 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.

#### Invited Lectures since 2000

1. Postquantum cryptology for group theorists, Group Theory Seminar, City University of New York, March 12, 2010.

2. Group-theoretic cryptology, Algebra Seminar, City University of New York, March 5, 2010.
3. Hard problems in group theory, International Conference on Geometric and Combinatorial Methods in Group Theory and Semigroup Theory, University of Nebraska, May 17-21, 2009
4. Group theory questions from cryptography, Group Theory Seminar, Centre de Recerca Matemàtica, Barcelona, January 26, 2009.
5. Generic case complexity and cryptography, IUMA Day on Cryptography, University of Zaragoza, January 23, 2009.
6. Randomized word problems, Session on Geometric Group Theory, Winter Meeting of the Canadian Mathematical Society, Ottawa, December 7, 2008.
7. Generic properties of finitely presented groups, AMS Special Session on Geometric Group Theory and Topology, Middletown, CT, October 12, 2008.
8. Group Theoretical Questions Motivated by Cryptography, Conf. on Combinatorial and Geometric Group Theory, Fairfield, CT, October 10, 2008.
9. Why Coset Enumeration Works, Group Theory: Generations, CUNY September 29, 2007.
10. The efficiency of group-theoretic algorithms, Centre de Recerca Matemàtica, Barcelona, October 10, 2007.
11. Generic case complexity and coset enumeration, Centre International de Rencontres Mathématiques, Marseille, March 2, 2007.
12. A zero–one law for finite subgraphs of Cayley graphs of groups, Centre de Recerca Matemàtica, Barcelona, September 28, 2006.
13. Generic complexity, Methods of Logic in Mathematics III, St. Petersburg, June 5, 2006.
14. Solving one variable equations in free groups, Special Session on Geometric Methods in Group Theory and Semigroup Theory, University of Nebraska, October 22, 2005.
15. Solving one variable equations in free groups, Special Session on Infinite Groups, Bard College, October 8, 2005.
16. Small cancellation conditions for semigroups, International Conference on Semigroups and Languages, Universidade de Lisboa, July 2005.
17. One variable equations over hyperbolic groups, Canadian Mathematical Society, Winter 2004 Meeting, Session on Groups, Equations, Non-commutative Algebraic Geometry, Mills University, December 11, 2004.
18. One variable equations over hyperbolic groups, Workshop on Geometric Group Theory, University of Newcastle, July 1, 2004.
19. Presentations of word hyperbolic groups, Special Session on Probabilistic and Asymptotic Aspects of Group Theory, Ohio University, March 27, 2004.

20. Equations over free and hyperbolic groups, Rutgers-Newark Colloquium, March 3, 2004.
21. The word problem for finitely presented groups, Conference on Computational Group Theory, City College of New York, September 25, 2003.
22. Formal languages and finitely presented groups, Oxford Algebra Seminar, March 2003.
23. Formal languages and word problems of groups, Newcastle Algebra Seminar, March 2003.
24. Approximating word problems of finitely presented groups, Edinburgh Algebra Seminar, February, 2003.
25. Computer science and group theory, Special Session on Interactions between Logic, Group Theory and Computer Science, Baltimore, January, 2003.
26. Constructing Cayley diagrams of groups, New York Group Theory Seminar, November, 2002.
27. Approximating word problems of groups, Special Session on Geometric Group Theory, Northeastern University, October, 2002.
28. Word problems, Workshop on the Elementary Theory of Free Groups and Related Topics, McGill University, August 2002.
29. Combinatorial group theory and formal languages, International Conference on Mathematical Logic, Algebra and Set Theory, Moscow, August 2001.
30. Automatic groups with counters, Conference on Finitely Presented Groups: Questions and Algorithms, Trento, July 2001.
31. Word hyperbolic semigroups, Workshop on Presentations and Geometry, Coimbra, July 2001.
32. Geometric Group Theory without Geometry (3 talks), Workshop on Groups and Languages, University of Neuchatel, Switzerland, June 2000.
33. Languages of Generators, Math 2000, McMaster University, Ontario, June 2000.
34. Groups with Context-Free Multiplication Table, International Conference on Geometric and Combinatorial Methods in Group Theory and Semigroup Theory, University of Nebraska, May 2000.
35. Reflections on Automatic Groups, Combinatorial Algebra Day, City College of New York, April 2000.
36. Automatic Quotients of Free Groups, New York Group Theory Seminar, March 2000.
37. Automatic Groups, Algebra Seminar, Temple University, March 2000.

#### **Other Recent Scholarly and Professional Activity**

1. Member of the editorial board of the journal *Groups, Complexity and Cryptology*, published by Heldermann-Verlag.

2. Member of the Eastern Section Program Committee of the American Mathematical Society, 2008-2008, Chair, 2008-2009.
3. Member of the editorial board of the Journal of Mathematical Cryptology, published by De Gruyter.
4. Founding member of the editorial board of the series Algorithms and Computation in Mathematics, published by Springer Verlag. (2003-2005).
5. Organizer of the Workshop on Generic Complexity held at the American Institute of Mathematics, Palo Alto, August, 2007.
6. Organizer of American Mathematical Society sectional meetings at Stevens, April 2007, and April 2001.