Clifford H. Bergman
Curriculum Vitae
November 2019

Current Address

Department of Mathematics
Iowa State University
Ames, Iowa 50011, USA

phone: 515–294–1752
fax: 515–294–5454
email: cbergman@iastate.edu

Home Address

3439 Buena Vista St.
San Diego, CA 92109, USA

cell: 515–451–7947

Education

B.S.	Brown University	1975
M.S., Ph.D.	University of California, Berkeley	1982

Professional Experience

2019–	Professor Emeritus, Iowa State University
2013–17	Chair, Department of Mathematics
2012–17	Barbara J. Janson Professor of Mathematics
2002–2019	Professor, Iowa State University
1987–2002	Associate Professor, Iowa State University
1993–94	Faculty Improvement Leave at University of Illinois, Chicago
1982–1987	Assistant Professor, Iowa State University
1981–1982	PostDoc, Univ. of Hawaii at Manoa

Research Interests

Universal Algebra, Logic, Algorithm Analysis, Cryptography, Steganography

Orcid ID: 0000-0002-1221-8459

Publications

BOOKS

1. *Universal algebra: Fundamentals and selected topics*, Taylor & Francis, ix+308pp., August 2011.
2. C. Bergman, R. Maddux, and D. Pigozzi (eds.), *Algebraic logic and universal algebra in computer science*, Lecture Notes in Computer Science, vol. 425, New York, Springer-Verlag, 1990.

IN PRINT/ACCEPTED

1. *Random models of linear idempotent Maltsev conditions, I, idemprimal algebras,* with Á. Szendrei, Algebra Universalis, to appear.
2. *Universal algebraic methods for constraint satisfaction problems,* with W. DeMeo, Logical Methods in Computer Science, to appear.
3. *Introducing Boolean semilattices*, Don Pigozzi on Abstract Algebraic Logic and Universal Algebra, Springer-Verlag, (2018), 103–130.
4. *Automorphism-primal algebras generate verbose varieties*, Algebra Universalis **74** (2015), no. 1, 117–122.
5. *Measuring bias in cyclic random walks*, with S. Sethuraman, Missouri J. Math. **25**, (2013), 195–212.
6. C. Bergman and D. Failing, *Commutative, idempotent groupoids and the constraint satisfaction problem*, Algebra Universalis **73** (2015), no. 3-4, 391–417.
7. *Fully invariant and verbal congruence relations*, with J. Berman, Algebra Universalis, **70**, (2013), 71–94.
8. *Computational complexity of generators and nongenerators in algebra*, with G. Slutzki, Int. Jour. Algebra and Computation **12** (2002), no. 5, 719–735.
9. *Computational complexity of some problems involving congruences on algebras*, with G. Slutzki, Theoret. Comp. Sci., **270** (2002), 591–608.
10. *Complexity of some problems concerning varieties and quasivarieties of algebras*, with G. Slutzki, SIAM Jour. of Comput. **30** (2000), no. 2, 359–382.
11. *Computational complexity of term-equivalence*, with D. Juedes and G. Slutzki, Int. Jour. Algebra and Computation **9** (1999), no. 1, 113–128.
12. *Categorical equivalence of modes*, with J. Berman, Discussiones Mathematicae **19** (1999), 41–62.
13. *Algorithms for categorical equivalence*, with J. Berman, Math. Struc. Comp. Sci. **8** (1998), 1–15.
14. *Categorical equvalence of algebras with a majority term*, Algebra Universalis **40** (1998), 149–175.
15. *Morita equivalence of almost-primal clones*, with J. Berman, J. Pure Appl. Algebra **108** (1996), 175–201.
16. *Subquasivarieties of regualarized varieties*, with A. Romanowska, Algebra Universalis **36** (1996), 536–563.

17. *Structural completeness in algebra and logic*, Algebraic Logic (H. Andréka, D. Monk, and I. Németi, eds.), Colloquia Mathematica Societatis János Bolyai, vol. 54, North-Holland, Amsterdam, 1991, pp. 59–73.

18. *Minimal varieties and quasivarieties*, with R. McKenzie, Journal of the Australian Math. Soc., Series A **48** (1990), 133–147.

19. *Non-axiomatizability of the amalgamation class of modular lattice varieties*, Order **6** (1989), 49–58.

20. *Residually small modular varieties with AP*, Houston J. Math. **14** (1988), 451–464.

21. *On the relationship of AP, RS, and CEP in congruence modular varieties, II*, with R. McKenzie, Proc. Amer. Math. Soc. **103** (1988), 335–343.

22. *Saturated algebras in filtral varieties*, Algebra Universalis **24** (1987), 101–110.

23. *On the relationship of AP, RS and CEP in modular varieties*, Algebra Universalis **22** (1986), 164–171.

24. *Amalgamation classes of some distributive varieties*, Algebra Universalis **20** (1985), 143–166.

25. *Deductive varieties of modules and related objects*, with L. Hogben, Trans. Amer. Math. Soc. **289** (1985), 303–320.

26. *The amalgamation class of a discriminator variety is finitely axiomatizable*, Universal Algebra and Lattice Theory (R. Freese and O. Garcia, eds.), Springer-Verlag, New York, 1983, Lecture notes in Mathematics, vol. **1004**, pp. 1–9.

27. *How to cancel a linearly ordered exponent*, with R. McKenzie and Zs. Nagy, Colloquia Mathematica Societatis János Bolyai, 29. Universal Algebra. Esztergom [Hungary], North-Holland Publishing Co., Amsterdam, 1977, pp. 87–93.

SUBMITTED

1. *Semilattice sums of algebras and Mal'tsev products of varieties,* with T. Penza and A. Romanowska.

2. *Joins and Maltsev products of congruence-permutable varieties.*

IN PREPARATION

1. *Random models off linear idempotent Maltsev conditions, II, simple, paraprimal, and pure majority algebras,* with A. Szendrei.

2. *Boolean fans*

3. *Congruence k-permutability of Maltsev products,* with J. Li.

4. *Categorical equivalence and central relations*, preprint, 1997.

5. *Boolean Krasner algebras*, preprint, 1996.

CONFERENCE PROCEEDINGS/EXTENDED ABSTRACTS (REFEREED)

1. *Joins and Maltsev Products of Congruence-Permutable Varieties,* Algebras and Lattices in Hawaii, 2018.

2. *An automatic, time-based, secure pairing protocol for passive RFID*, with George T. Amariucai and Yong Guan, RFID. Security and Privacy, Lecture Notes in Computer Science, vol. 7055, Springer-Verlag, 2012, pp. 108–126.

3. *An artificial neural network for wavelet steganalysis*, with J. Davidson and E. Bartlett, Optics and Photonics, Mathematical Methods in Pattern and Image Analysis, vol. 5916, SPIE, 2005, pp. 1–10.

4. *Unitary embedding for data hiding with the SVD*, with J. Davidson, Security, Steganography and Watermarking of Multimedia Contents VII, SPIE, 2005.

5. *Computational complexity of some problems involving congruences on algebras*, With G. Slutzki, Fifteenth Annual IEEE Symposium on Logic in Computer Science (Los Alamitos, CA), IEEE, IEEE Computer Society, 2000, pp. 168–174.

6. *Complexity of some problems in universal algebra*, with G. Slutzki, 16th Symposium on Theoretical Aspects of Computer Science (STACS '99) (Berlin) (C. Meinel and S. Tison, eds.), Lecture Notes in Computer Science, vol. 1563, Springer-Verlag, 1999, pp. 163–172.

OTHER PUBLICATIONS

1. *ANNTS: artifical neural network technology for steganalysis*, with E. Bartlett et al.

2. *An artificial neural network for wavelet steganalysis*, Tech. report, Midwest Forensics Resource Center, 2007, with J. Davidson.

3. *MFRC stego database*, 2 DVD discs, 2006, Available from Ames Laboratory, Iowa State University, Ames, Iowa 50011.

4. *Proposed construction of a card verification number*, Tech. report, Von Maur Department Stores, March 2005.

5. *A survey of available cryptosystems*, Tech. report, Science Applications International Corporation, 2004, Originally written for International Simulation and Training Systems, Ltd., 2002.

6. *Revitalizing engineering calculus at Iowa State University*, with E. Johnston, J. Mathews and A. Heckenbach, in "The Laboratory Approach to Teaching Calculus" (L. Leinbach et al., eds.), MAA Notes, vol. 20, Mathematical Association of America, 1991, pp. 169–186.

7. *Algebraic logic and universal algebra in computer science*, edited with R. Maddux and D. Pigozzi, Lecture Notes in Computer Science, vol. 425, New York, Springer-Verlag, 1990.

8. *Concerning the amalgamation bases of congruence distributive equational classes*, University of California, Berkeley, 1981, Ph.D. Thesis.

External Funding

1. *Collaborative research: algebra and algorithms, structure and complexity theory,* NSF, Sept. 2015–Aug. 2018, $99,881. REU Supplement, June 2016, $7,000.

2. *REU Site: Iowa State University Mathematics REU,* with L. Hogben, National Science Foundation, Feb. 2015–Jan. 2020, $348,115.

3. *Information Assurance Scholarship for Service,* with D. Jacobson, B. Licklider, J. Wiersma and J. Wong, National Science Foundation, Aug. 2013–July 2018, $2,182,241.

4. *SFS Scholarships for Information Assurance Students,* with D. Jacobson, B. Licklider, J. Wiersma and J. Wong, National Science Foundation, Aug. 2009–July 2012, $1,956,130.

5. *SFS Scholarships for Information Assurance Students,* with D. Jacobson, B. Licklider, J. Wiersma and J. Wong, National Science Foundation, Aug. 2005–July 2009, $888,008.

6. *An Artifical Neural Network for Wavelet Steganalysis,* Midwest Forensics Resource Center, $79,000 with J. Davidson,

7. *Cyber Protection Lab,* Industry/University Cooperative Research Center planning grant, National Science Foundation, August 2002, $10,000, with D. Jacobson, et al.

8. *SFS Fellowships for Information Assurance Students,* NSF-0113552, July 2001–June 2005, $2,626,026, PI (with J. Davis, D. Jacobson, C. Miller and J. Wong).

9. *Information Assurance Educational Support Program,* NSF-0113549, July 2001–June 2003, $199,998, PI (with J. Davis, D. Jacobson, S. Schmidt and J. Wong).

10. *Integrated Security Curricula Modules,* NSF EIA-9979985, Sept. 1999–Aug. 2002, $387,136, PI (with J. Davis, D. Jacobson, S. Russell and J. Wong).

11. *Conference on Applications of Universal Algebra and Algebraic Logic to Computer Science,* Institute for Mathematics and its Applications, Jan–June 1988, $1000, PI.

12. *Conference on Applications of Universal Algebra and Algebraic Logic to Computer Science,* Office of Naval Research, N00014–88–J–1182, Jan–June 1988, $2392, PI (with R. Maddux and D. Pigozzi).

13. *Conference on Applications of Universal Algebra and Algebraic Logic to Computer Science,* NSF CCR-8800793, Jan.–June 1988, $4000, PI (with R. Maddux and D. Pigozzi).

14. *Problems in Universal Algebra,* National Science Foundation (NSF), DMS8701643, 1987–89, $45,175, Sole PI.

Colloquia, Conference and Workshop Presentations

A. Plenary conference talks

1. BLAST2015, at University of Texas, Dallas, June 2015.
2. Plenary address at Colloquium on Universal Algebra, Szeged, Hungary, 1989

B. Invited, externally funded, conference and workshop talks

1. Structure and Complexity in Universal Algebra, Vanderbilt University, June 2016
2. Algebra and Algorithms, Univ. Colorado, Boulder, May 2016
3. First Thomasina Coverly Memorial Workshop on Universal Algebra and Ordered Sets, Vanderbilt University, May 2000
4. Regional meeting of the Canadian Mathematical Society, Kingston, Ontario, Dec. 1998
5. Conference on Modes, Modals and Related Structures, Warsaw, Poland, March 1997
6. Fields Institute for the Mathematical Sciences, Nov. 1996
7. Conference on Algebraic Logic, Budapest, Hungary, August 1988

C. Other invited conference and workshop talks

1. Special Session on Algebra and Algorithms, American Mathematical Society, Denver, Jan. 2020.
2. Algebras and Lattices in Hawaii, 2018.
3. Special Session in Algebras, Lattices, and Varieties, American Mathematical Society, College of Charleston, March 2017.
4. Special Session in Algebraic Logic, American Mathematical Society, Univ. Denver, Oct. 2016.
5. Open Problems in Universal Algebra. A Shanks Workshop, Vanderbilt University, 2015.
6. General Algebra and Its Applications, University of Melbourne, Australia, 2013.
7. Conference on Universal Algebra and Lattice Theory, Szeged, Hungary, June 2012.
8. Regional meeting of the American Mathematical Society, St. Paul, MN, April 2009.
9. Regional meeting of the American Mathematical Society, Urbana-Champaign, IL, March 2008.
10. Annual meeting of the Midwest Forensics Resource Center, Ames, Iowa, June 2005.
11. Regional meeting of the American Mathematical Society, Nashville, TN, Oct. 2004.
12. Annual meeting of the Association of Symbolic Logic, Chicago, Illinois, June 2003.
13. Molokai Conference on Universal Algebra and Lattice Theory, Molokai, Hawaii, January, 1987
14. Asilomar Conference on Algebras, Lattices and Logic, July 1987

D. Contributed conference and workshop talks

1. Annual meeting of SPIE, San Diego, August 2005.
2. Logic in Computer Science (LICS 2000), Santa Barbara, June 2000
3. Regional meeting of the American Mathematical Society, Louisville, KY, March 1998

4. International Conference on Modern Algebra and Its Applications, Vanderbilt University, May 1996
5. Conference on Universal Algebra, Karlovy Vary, Czechoslovakia, August 1988
6. National Institutes of Health Conference on Universal Algebra and Lattice Theory, Bethesda, MD, August 1986
7. Fourth International Conference on Universal Algebra and Lattice Theory, Puebla, Mexico, January 1982

E. Remunerated talks at other institutions

1. University of Waterloo, Waterloo, Ontario, Jan. 2006
2. Winona State University, Winona, MN, Nov. 2005
3. University of Illinois, Chicago, Nov. 1988

F. Other talks

1. Truman State, Oct. 2011
2. Concordia College, Oct. 2008
3. Univ. Nebraska, Omaha, Oct. 2008
4. Univ. South Dakota, Nov. 2007
5. Information Assurance Student Group, ISU, April 2007
6. Winona State, Nov. 2005
7. College of Engineering, ISU, Oct. 2005
8. Morningside College, February 2005
9. Univ. Wisconsin, Stout, February 2005
10. Luther College, February 2004.
11. Buena Vista College, February 2004.
12. Truman State College, November 2003.
13. Department of Computer Science, ISU, October 2000.
14. Maharishi University of Management, April 2000.
15. Harvey Mudd College/U. C. Riverside, Dec. 1994

Graduate Recruitment Talks

1. Concordia College, Oct. 2008
2. Univ. Nebraska, Omaha, Oct. 2008
3. Univ. South Dakota, Nov. 2007
4. Winona State, Nov. 2005
5. Morningside College, February 2005
6. Univ. Wisconsin, Stout, February 2005
7. Luther College, February 2004.
8. Buena Vista College, February 2004.
9. Truman State College, November 2003.
10. Maharishi University of Management, April 2000.

Educational Activities

30 years experience teaching mathematics in both large and small classes, including

Undergraduate: algebra and trigonometry, calculus, differential equations, abstract algebra, linear algebra, number theory, probability and statistics;

Graduate: abstract algebra, universal algebra, set theory, cryptography.

Between 1997 and 2008, my course in cryptography was been videotaped and offered for graduate credit to in-service professionals through Iowa State's Engineering Distance Education Program and National Technological University. A considerable amount of material I prepared for the class is available by request.

Curriculum Development

- Member of the faculty for the certificate program in Information Assurance, ISU
- Designed a graduate level course in cryptography that is offered to approximately 50 students each year via both classroom presentation and videotape.
- Helped design a computer-enhanced calculus sequence for undergraduates
- Designed course in Universal Algebra and wrote extensive notes (available upon request)

Teaching Awards and Recognition

1. Designated as "Most influential teacher" by two Iowa State math majors at the annual Student Scholars and Leaders Recognition Ceremony (Jason Juett and Kaeli Samson), 2005.
2. Master Teacher, College of Liberal Arts and Sciences, Iowa State University, 2004.
3. Vinograde Award for Outstanding Graduate Advising, Department of Mathematics, Iowa State University, 2004.
4. Vinograde Award for Outstanding Graduate Teaching, Department of Mathematics, Iowa State University, 2001.
5. University Teaching Award, $1,000, Dec. 1989, Iowa State University.

Ph. D. Students

1. Jiali Li, May 2017, *Congruence n-permutaboe varieties.*
   Employment History
   2017– Affinity inc., Washington D.C. (Data analytics)

2. David Failing, Ph.D. May 2014, *Commutative, Idempotent Groupoids and the Constraint Satisfaction Problem.*
   Employment History
   2017–present Assistant Professor (tenure track), Lewis University
   2014–2017 Assistant Professor (tenure track), Quincy College
   2013–14 Graduate Program in Informatics, Univ. Illinois Urbana-Champaign

3. Elizabeth Kleiman, Ph.D. (Math-ComS) August 2010, *High Performance Computing Techniques for Attacking Reduced Versions of AES using the XL and XSL methods.*
   Employment History
   2010–present Associate Professor of Mathematics and Computer Science,
   Mt. Mercy University.

4. Kristin Meyer, Ph.D. May 2006, *A New Message Authentication Code Based on the Non-associativity of Quasigroups.*
   Employment History
   2006–present Associate Professor, Wisconsin Lutheran College

5. Mandy Maxwell, Ph.D. May 2005, *Almost Perfect Nonlinear Functions and Related Combinatorial Structures* (Co-major professor with Sung Yell Song. Song did all of the work.)
   Employment History
   2005– Associate Professor, Trinity Christian University.

6. Sergei Babyonyshev, Ph.D. August 2004, *Metatheories of Deductive Systems.* (Co-major professor with Don Pigozzi. Pigozzi did all of the work.)
   Employment History
   current position Asst. Prof. Siberian Fire-Rescue Academy.

7. Joy Becker, Ph.D. May 2002, *Computational Complexity of Digraph Decomposition and the Congruence Extension Property for Algebras.*
   Employment History
   2010– Associate Professor, Wartburg College
   2002–2010 Associate Professor, University of Wisconsin, Stout

8. Pamela Reich, Ph.D. Dec. 1996, *Complex Algebras of Semigroups*.
   Employment History
   2000– Professor, Truman State University
   1996–2000 Assistant Professor, Drury College

9. Hernando Gaitán, Ph.D. August 1990, *Quasivarieties of p-algebras and Wajsberg algebras*.
   Employment History
   ??– Universidad Nacional de Colombia
   1990–?? Universidad de los Andes, Merida, Venesuala

M.S. Students

1. Robert Perry, December 2017. Last known position: unknown.
2. Nuwan De Silva, December 2013. Last known position: software engineer.
3. Josh Lagrange, summer 2012. Last known position: unknown.
4. Lauren Hermann, May 2012. Last known position: data analyst, Cabela's Inc.
5. Jody Tomjack (MSM), Fall 2011. Last known position: high school teacher in Sioux Falls
6. Sahnghyun Cha (Computer Sci.), Fall 2010. Last known position: Ph.D. student at U. Virginia
7. Jason Kline, summer, 2010. Last known position: instructor at Northern Iowa Community College
8. Jonathan Wrolstad, May 2009. Last known position: classified
9. Bryce Allen, Dec. 2008. Last known position: Software Engineer
10. Andrew Reginscheid, May, 2007. Last known position: Research scientist, NIST
11. Elizabeth Kleiman, August, 2005. Last known position: Associate Professor of Mathematics and Computer Science, Mt. Mercy College, Cedar Rapids, Iowa.
12. Christy Stanley, August, 2005. Last known position: Price-Waterhouse Coopers
13. Tim Dewey, May, 2005. Last known position: National Security Agency
14. Christie Shuster, May 2004. Last known position: National Security Agency.
15. Ryan Swanstrom, May 2003. First job: security engineer for Northrup-Grumann, Omaha, Nebraska.
16. Stefan Rothbauer, July 2002. First job: student at University of Augsburg, Germany.
17. Gregory Gross, April 2002. First job: high-school teacher in Omaha.
18. Anneke Stellmacher, July 2000. First job: student at University of Augsburg, Germany.
19. Amy Hoover, May 1999. Last known position: unknown.
20. David Mitchell, Dec. 1998. Last known position: Lecturer and Varsity Wrestling Coach: Luther College.
21. Pam Reich, May 1993. Last known position: Professor, Truman State University.
22. Paul Hertzel, May 1992. Last known position: Northern Iowa Community College.
23. Lois Thur, June 1991. First job: Concordia University.
24. Kathy Rogotzke, June 1990. First job: Northern Iowa Community College.
25. Richard Flint, June 1990. Last known position: unknown.
26. Laura Smith, June 1988. Last known position: California State University, Monterey Bay
27. Joyce Beckman, M.S. Dec. 1986. Current employment: University of Southern Indiana.

Undergraduate Students

Undergraduate Honors Project	Leslie Lippitt[1], 2004
	Kristine Stacey, 1992
Undergraduate Thesis	Leslie Miller, 2000
Independent Study	Donald Peterson, 2008
	Nathan Brace, 2006
	Niloy Ray, 2001
	Patrick Breheny, 2001
REU Program	Mentor 2005

Professional Activities

- Organized and moderated a "birds-of-a-feather" session on the teaching of cryptotgraphy at CRYPTO 2003.
- Mentor for group of high school students from Humboldt County competing in *Adventures in Supercomputing,* Spring 2000.
- Pari-GP is a library of routines for doing computations in algebraic number theory. (GP is the interactive front-end.) I am helping develop the documentation for this project. Most of the software originated at the University of Bordeaux. (See `http://pari.math.u-bordeaux.fr/`)
- Together with Drs. Maddux and Pigozzi, organized a conference, held at ISU, from June 1–4, 1988. The conference on Algebraic Logic and Universal Algebra in Computer Science included 8 invited speakers and attracted 76 participants. The proceedings were published by Springer-Verlag. Our meeting spawned a series of similar conferences, collectively known as AMAST (Algebraic Methodology and Software Technology).

Information Assurance Center

- I am a member of the Advisory Board of the Information Assurance Center.
- Founding member of both the Iowa State Information Systems Security Lab (ISSL) and the Iowa State Information Assurance Center (IAC). The Center has been designated one of 23 "Centers of Excellence in Information Assurance" by the National Security Agency.
- Co-PI of the grant and a member of the panel administering the Iowa State "CyberCorps". This is a training program for undergraduate and graduate students in Information Assurance. It involves a two-year scholarship, leadership training, summer internship and placement with a Federal agency upon graduation. The program is funded by the National Science Foundation.
- Organizer of the Information Assurance Colloquium. This is a University-wide forum for the discussion of a wide variety of issues related to computer and information security. Although several of the speakers have been members of the Iowa State Community, most are visitors from industry and government.

[1] Leslie's project won the award for best LAS honors project in 2004

- Starting in 2004, the Center has offered a 3-day summer camp in computer security for high school students. I am one of the instructors for the camp.
- The Center has spawned an NSF-sponsored industry/university cooperative called the Center for Information Protection (`http://www.iac.iastate.edu/Research/CIP.html`). The CIP consists of 3 Universities and about a dozen industrial partners. Initial funding is $1,000,000.
- The Information Assurance Courseware Evaluation Program has recertified Iowa State as meeting all of the elements of the Committee on National Security Systems Training Standard for INFOSEC Professionals, No. 4011 and 4013. We received the highest rating.

Other Departmental and University Activities

- I served as Chair of the Department of Mathematics from July 2013 through August 2017.
- I have served on virtually every departmental committee including the undergraduate and graduate curriculum comittees, promotion and tenure committies, qualifying exam and search committees. Furthermore, I have frequently chaired those committees.
- Chair of the Mathematics Department Advisory Committee, 2005–7. The committee's duties cover all responsibilities not specifically delegated to the department chair or associate chairs.
- I served as Chair of the College of Liberal Arts and Sciences Promotion and Tenure Committee 2007–2011.
- At the University level, I have served as departmental representative to the College Senate, served on the Faculty Conduct Review Board, a conflict of interest oversight committee, Faculty Senate P&T Task Force, among other assignments.

Outreach Activities

- Consulted with Von Maur Department Stores on the design of a "Credit Card Verification Number" system. (March 2005).
- Instructor in the Computer Security Summer Camp offered to high-school students through the Information Assurance Center. The camp is funded by the State of Iowa Department of Administrative Services.
- Participated in the Information Assurance Educational Support Program. This is a 2-day workshop offered to faculty at midwestern colleges and universities interested in offering their own courses in computer security.
- Iowa Master Gardener and a Reiman Garden co-hort.