



CV and Bibliography

Name: Tanush Shaska

Address: 546 Science and Engineering Building,
Department of Mathematics and Statistics,
Oakland University, Rochester, Michigan, 48309.

Phone: (office) 248-370-3436

E-mail: shaska@oakland.edu
<http://www.oakland.edu/~shaska>

Birthplace: Vlora/Albania

Citizenship: USA

Research areas

Computational algebraic geometry, moduli spaces of curves, invariant theory, theta functions, mathematics of communications, coding theory, and cryptography.

Education

1996-01 Ph.D. Mathematics, University of Florida

1992-94 B.S. Mathematics, University of Michigan (Highest Distinction)

Employment

2008- *Associate Professor of Mathematics*, Oakland University

2008- *Rector*, University of Vlora.

2008- *Professor of Mathematics (Adjunct)*, University of Vlora.

2005-07 *Assistant Professor of Mathematics*, Oakland University

Summer 07 *Visiting Professor*, Department of Computer Science,
Maria Curie-Sklodowska University, Lublin, Poland

2003-05 *Assistant Professor of Mathematics*, Department of Mathematics, University of Idaho

2001-03 *Visiting Assistant Professor of Mathematics*, Department of Mathematics,
University of California at Irvine

2000 *Deutsche Forschungsgemeinschaft Fellow*, Department of Mathematics,
University of Erlangen, Germany.

1996-99 *Graduate Teaching Assistant*, Department of Mathematics, University of Florida

1995-96 *Consultant/Programmer*, Computer Business Solutions Inc., Farmington Hills, MI

Professional Activities

- *Editor in Chief:* Albanian Journal of Mathematics
- *Director:* NATO Advanced Study Institute,
New challenges in digital communications, Vlora, Albania, 2008.
- *Scientific committee:* Kazimierz Dolny Conference in complex systems, Poland.
- *Scientific committee:* Vlora Conference Series
- *Guest Editor:* Serdica Journal of Computing
Special issue on "Coding theory and cryptography", 2007.
- *International Scientific Board of Applications of Computer Algebra (ACA)*

Grants

- 2008-13 Computational Science Training for Undergraduates in the Mathematical Sciences **(PI)**, Algebraic curves and their applications in coding theory and cryptography, NSF 06-559, \$ 706 000.
- 2007-08 Nato Advanced Study Institute **(PI)**, 62 000 Euro
New challenges in digital communications, ICS.EAP.ASI No.982903.
- 2007-08 Albanian Ministry of Sciences **(PI)**, 15 000 Euro
New challenges in digital communications.
- 2007 NSF Conference grant **(PI)**, NSF 05-540 \$ 6 000
- 2005 NSA Conference grant **(PI)**, \$ 15 500
- 2004-05 Outreach program, University of Idaho, \$ 30 500
- 2004 NSF-Epscor grant **(PI)** S0511, \$ 10 000
- 2000 German Academy of Sciences, DFG, DM 24 000

Conferences organized

- 2009 Co-organizer: AMS Special Session on Computational Algebraic and Analytic Geometry for Low-Dimensional Varieties. AMS annual meeting, (with M. Seppala and E. Volcheck), Washington DC, January 2009.
- 2008 General Chair: Nato Advanced Study Institute,
New challenges in digital communications, Vlora, Albania, 2008.
- 2007 General Chair: Applications of Computer Algebra, ACA 2007, supported by NSF.
July 2007, Oakland University, Rochester, MI.
- 2007 Co-organizer: Vlora conference in algebra, coding theory, and cryptography,
(with A. Elezi), May 2008, Vlora, Albania.
- 2007 Co-organizer: Special session in coding theory, ACA 2007, supported by NSF,
(with D. Joyner and C. Shor), Oakland, MI.
- 2007 Co-organizer: Special session in computational algebraic geometry, supported by NSF,
(with A. Elezi), Oakland, MI.
- 2007 Co-organizer: AMS Special Session on Computational Algebraic and Analytic Geometry for Low-Dimensional Varieties. AMS annual meeting,
(with M. Seppala and E. Volcheck), New Orleans, January 2007.
- 2006 Co-organizer: Coding theory and cryptography,
(with S. Dodunekov), Varna, Bulgaria, 2006.
- 2005 Organizer: Computational aspects of algebraic curves, supported by NSA,
Moscow, Idaho, 2005.
- 2005 Co-organizer: *Special Session on Algorithmic Algebraic and Analytic Geometry*
AMS annual meeting,
(with M. Seppala and E. Volcheck), Atlanta 2005.
- 2004 Organizer: Special session: *Computational aspects of algebraic curves*, ACA 04
Applications of Computer Algebra, ACA 2004, Beaumont, TX.
- 2003 Organizer: Special session: *Computational aspects of algebraic curves*,
Applications of Computer Algebra, ACA 2003, NC State, Raleigh, NC.
- 1999-01 Organizer: The mathematical olympiad *E vërteta*, Vlora, Albania.

Selected honors and awards

- 2006 Department Merit Award, Department of Mathematics, Oakland University.
- 2000 Deutsche Forschungsgemeinschaft Fellow, German Academy of Sciences.
- 2001 Threadgill Dissertation Fellowship, College of Arts and Sciences, University of Florida
- 1994 Graduated with high distinction, University of Michigan
- 1985 First prize of the mathematical olympiad, Vlora (Albania)

Selected visiting institutions

Mathematical Sciences Research Institute, Berkeley
Institute of Mathematics and Applications, IMA, Minnesota
Institut für Experimentelle Mathematik, Essen, Germany
Universität Erlangen-Nürnberg, Germany
University of Heidelberg, Germany
Boston University, Boston
Universidad de Cantabria-Santander, Spain
UMCS, Lublin, Poland
University of Vlora, Albania

Graduate students

- Lubjana Besha
- R. Sanjeeva (PhD candidate) Thesis problem: Automorphism groups of algebraic curves over finite fields.
- G. Wijesiri, PhD Thesis: Theta functions and algebraic curves with automorphisms, Graduated: March 2008.

Reviewing/Refereeing

NSF grant reviewer
NSA grant reviewer
Mathreviews (over 20 math articles reviewed)
Forum Math.
Albanian J. Math.
Applicable Algebra In Engineering, Communication and Computing
Contemporary Math.
Serdica Journal of Computing

Publications

Articles and preprints

1. On the homogeneous algebraic graphs of large girth and their applications *Linear Algebra and its Applications*, (with V. Ustimenko), *Linear Algebra and Appl.* (to appear)
2. Codes over rings of size p^2 and lattices over imaginary quadratic fields, (with C. Shor, G. Wijesiri), *Finite Fields Appl.*, (to appear).
3. Quantum codes from algebraic curves with automorphisms, *Condensed Matter Physics*, 2008, vol. 11, No. 2(54), p. 383-396.
4. Genus 2 curves that admit a degree 5 map to an elliptic curve, (with K. Magaard, H. Völklein), *Forum Math.*, (to appear)
5. Codes over rings of size four, Hermitian lattices, and corresponding theta functions, (with S. Wijesiri), *Proc. Amer. Math. Soc.*, 136 (2008), 849-960.
6. Thetanulls of cyclic curves of small genus, (with E. Previato and S. Wijesiri), *Albanian J. Math.*, Special issue on computational algebraic geometry, **vol. 1**, Nr. 4, 2007, pg. 265-282.
7. Some open problems in computational algebraic geometry, *Albanian J. Math.*, Special issue on computational algebraic geometry, **vol 1**, Nr. 4, 2007, 309-321.

8. Codes over F_{p^2} and $F_p \times F_p$, lattices, and theta functions. (with C. Shor), *Advances in Coding Theory and Cryptology*, vol 3. (2007), pg. 70-80.
9. On the automorphism groups of some AG-codes based on C_{ab} curves, (with Q. Wang), *Serdica Journal of Computing*, 2007, vol. 1. pg. 193-206.
10. Hyperelliptic curves with reduced automorphism group A_5 , (with D. Sevilla), *Appl. Algebra Engrg. Comm. Comput.*, (2007), vol. 1, pg. 3-20.
11. Subvarieties of the hyperelliptic moduli determined by group actions, *Serdica Math. Journal*, **No. 4**, 2006, pg. 355-374.
12. Hyperelliptic curves with extra involutions, (with J. Gutierrez), *LMS J. of Comput. Math.*, 8 (2005), 102-115.
13. Galois groups of prime degree polynomials with nonreal roots, (with A. Bialostocki), *Lect. Notes in Computing*, vol 13. (2005), pg. 231-245.
14. A Maple package for hyperelliptic curves, (with S. Zheng), Ed. I. Kotsieras, Maple conference, 2005, pg. 161-175.
15. Hyperelliptic curves of genus 3 with prescribed automorphism group (with D. Sevilla and J. Gutierrez), *Lect. Notes in Computing*, vol 13. (2005), pg. 201-225.
16. Genus 2 curves covering elliptic curves, a computational approach, *Lect. Notes in Computing*, vol 13. (2005), pg. 151-195.
17. On the generic curves of genus 3, (with J. L. Thompson), *Contemporary. Math.*, Vol. **369**, pg. 233-244, AMS, 2005.
18. Invariants of binary forms (with V. Krishnamorthy and H. Völklein), *Developments in Mathematics*, Vol. 12, Springer 2005, pg. 101-122.
19. Some special families of hyperelliptic curves, *J. Algebra Appl.*, vol **3**, No. 1 (2004), 75-89.
20. Genus 2 fields with degree 3 elliptic subfields, *Forum. Math.*, vol. **16**, 2, pg. 263-280, 2004.
21. Elliptic subfields and automorphisms of genus two function fields, (with H. Völklein) *Algebra, Arithmetic and Geometry with Applications. Papers from Shreeram S. Abhyankar's 70th Birthday Conference*, pg. 687 - 707, Springer (2004).
22. Computational algebra and algebraic curves, ACM, *SIGSAM Bulletin, Comm. Comp. Alg.*, Vol. **37**, No. 4, 117-124, 2003.
23. Computational aspects of hyperelliptic curves, Computer mathematics. Proceedings of the sixth Asian symposium (ASCM 2003), Beijing, China, April 17-19, 2003. River Edge, NJ: World Scientific. *Lect. Notes Ser. Comput.* 10, 248-257 (2003).
24. Determining the automorphism group of a hyperelliptic curve, *Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation*, ACM Press, pg. 248 - 254, 2003.
25. The locus of curves with prescribed automorphism group. (with K. Magaard, S. Shpectorov, and H. Völklein) *Communications in arithmetic fundamental groups* (Kyoto, 1999/2001). Sūrikaiseikikenkyūsho Kōkyūroku No. 1267 (2002), 112-141.
26. Genus 2 curves with (3,3)-split Jacobian and large automorphism group, Algorithmic Number Theory (Sydney, 2002), **6**, 205-218, *Lect. Not. in Comp. Sci.*, 2369, Springer, Berlin, 2002.
27. Curves of genus 2 with (n, n) -decomposable Jacobians, *J. Symbolic Comput.* 31 (2001), no. 5, 603-617.

Books edited or authored

1. **New challenges in communications**, NATO ASI, T. Shaska, E. Hasimaj, ISO Press, 2008 (to appear)
2. **Advances in coding theory and cryptology**, Series: *Coding Theory and Cryptography*, vol **3**, T. Shaska, W. C. Huffman, D. Joyner, V. Ustimenko (Eds), World Scientific, 2007.
3. **Computational aspects of algebraic curves**, Lecture Notes in Computing Series, T. Shaska (Ed), World Scientific, vol. **13**, (2005), 288pp, ISBN 981-256-459-4.
4. **Progress in Galois Theory, Proceedings of J. Thompson's 70-th birthday**, Series: *Developments in Mathematics*, Vol. **12**, H. Völklein, T. Shaska (Eds.), Springer, 2005, X, 168 p., Hardcover ISBN: 0-387-23533-7.
5. **Kurbat Algjebrike**, (Albanian), AulonnaPress, 2005, 165 p., Softcover, ISBN 0-9754541-1-0.
6. **Lecture Notes in Linear Algebra**, T. Shaska, AulonnaPress, 2004, xii+192 pp., ISBN 0-9754541-0-2.
7. **Algjebra Lineare**, T. Shaska, AulonnaPress, 2004, xii+248 pp.

Selected Talks

1. Algebraic curves of small genus and their automorphisms, Discrete Math Colloquium, University of Delaware, March 2008.
2. Genus 2 curves covering elliptic curves, Simon Fraser University, Oct. 2007.
3. Equations of curves with automorphisms, AMS Special session, DePaul University, Oct. 2007.
4. Some historical remarks on automorphisms of algebraic curves, Department of Mathematics and Statistics, Colloquium, Oakland University, Oct. 2007.
5. Remarks on some old problems of algebraic geometry, Michigan Tech. University, Sep. 2007
6. *Moduli spaces of curves and theta functions*, Vlova conference in Algebra, Coding Theory, and Cryptography, Vlova, Albania, May 26-27, 2007.
7. *A historical view of theta functions*, University of Lublin, Poland, May 2007.
8. *Theta functions and algebraic curves with automorphisms*, Algebra Seminar, Wayne State University, February 7, 2007.
9. *Theta functions and algebraic curves*, Math Colloquium, Oakland University, Fall 2006.
10. *Codes over rings of size four, lattices, and their theta functions*, University of Lublin, Poland, Fall 2006.
11. *Some open problems in computational geometry*, University of Michigan-Dearborn, Fall 2006.
12. *Theta functions and automorphism groups of curves*, Galoistheorie Kolloquium, Institut für Experimentelle Mathematik (IEM), Essen, Germany, 2006.
13. *Theta functions and application to coding theory*, ACA 2006, Varna, Bulgaria, 2006.
14. *Invariants of binary forms*, Math Colloquium, Oakland University, Winter 2006.
15. *Algebraic curves and their applications in engineering*, Sigma-Chi society, Oakland Univ. Fall 2005.
16. *Algebraic varieties associated to network coding*, Wayne State University, Fall 2005.

17. *Hyperelliptic curves with reduced automorphism group A_5* , AMS Western section, Santa Barbara, April 2005.
18. *Genus 2 curves that admit a degree 5 map to an elliptic curve*, Joint AMS meeting, Atlanta, January 2005.
19. *Genus 2 curves with $(5, 5)$ split Jacobian*, Institute for Experimental Mathematics, Essen, Germany, December 2004.
20. *Field of moduli of curves, a computational approach*, Workshop Computational Arithmetic Geometry, PIMS SFU, July 5 - 9, 2004.
21. *On the field of moduli of curves*, Algebra seminar, Wayne State University, April 2004.
22. *Genus 2 curves with degree 5 elliptic subcovers*, **991-14-21 AMS**, Southeastern Section Meeting, Chapel Hill, October 2003.
23. *Determining the automorphism group of algebraic curves*, ISSAC 03, Drexler University, Philadelphia, August 2003.
24. *Computational aspects of hyperelliptic curves*, ACA 03, Raleigh, NC, July 2003.
25. *The monodromy group of a generic curve covering \mathbb{P}^1* , Joint International Meeting of AMS and RSME, Seville, Spain, June 2003.
26. *Computational aspects of hyperelliptic curves*, University of Cantabria, Santander, Spain, June 2003.
27. *Loci of hyperelliptic curves with prescribed group action*, Computational Aspects of Algebraic Curves, and Cryptography, Gainesville, 2003.
28. *Hyperelliptic curves with non-hyperelliptic involutions* **983-14-115 AMS**, Joint Mathematics Meeting, Baltimore, January 2003.
29. *Hyperelliptic curves with extra automorphisms*, Galois Theory Conference, John Thompson's 70th birthday, Gainesville 2002.
30. *Field of definition and field of moduli of hyperelliptic curves*, University of Florida Colloquium, Gainesville, Florida, September 2002.
31. *Computational aspects of algebraic geometry*, Algebra seminar, UC Irvine, CA, December 2002.
32. *Genus 2 curves with $(3,3)$ -split Jacobian and large automorphism group*, ANTS V, International Symposium in Algorithmic Number Theory, Sydney, 2002.
33. *Automorphisms and elliptic subfields of genus 2 fields* (with H. Völklein), **972-14-47 AMS**, Southwestern Conference, Groups and Covering Spaces in Algebraic Geometry, Irvine, CA, November 2001.
34. *The automorphism group of a Riemann surface*, University of Florida Colloquium, Gainesville, Florida, September 2001.
35. *Elliptic subfields and automorphisms of genus 2 curves*, University of Erlangen, Germany, June 2001.
36. *Computing the locus of genus 2 fields with degree 2 or 3 elliptic subfields*, Institute for Experimental Mathematics, Essen, Germany, May 2001.
37. *Some Computational Aspects of Genus 2 Curves*, Number Theory Conference, University of Illinois, Urbana-Champaign, IL, May 2001.
38. *Genus 2 curves covering elliptic curves*, Workshop on Arithmetic Geometry, MSRI, Berkeley, CA, December 2000.

39. *Modular curves and Hurwitz spaces*, Conference on Topological Groups, TU-München, Germany, June 2000.
40. *Curves of genus two with (n,n) -decomposable Jacobians*, AG Gruppentheorie, Erlangen, Germany, March 2000.
41. *Explicit equation of certain Hurwitz spaces*, University of Heidelberg, Germany, May 1999.
42. *Curves of genus 2 covering elliptic curves* (with V. Krishnamoorthy), **940-12-287 AMS**, Southeastern Conference, Gainesville, Florida, March 1999.
43. *Rigid tuples and monodromy groups*, Conference on ABC-conjecture, Tucson, Arizona, March 1998.

Teaching:

Graduate courses:

Algebraic Geometry, MTH 671, Oakland University, Winter 08
 Algebra I, MTH 571, Oakland University, Fall 05, Fall 06
 Algebra II, MTH 572, Oakland University, Winter 07
 Coding Theory, APM 673, Oakland University, Winter 06
 Algebraic geometry methods in engineering, APM 505, Oakland Univ., Sum. 06
 Topics in Cryptology, APM 505, Oakland University, Sum. 05
 Graph Theory and Combinatorial Math, APM 563, Oakland University, Fall 05
 Computer Security and Cryptography, Math 504, Univ. of Idaho, Sp. 05
 Galois Theory, Math 553, Univ. of Idaho, Sp. 04
 Group Theory, Math 552, Univ. of Idaho, Fall 03

Undergraduate courses:

Abstract Algebra, APM 475, Oakland University, Winter 07, 08
 Linear Algebra, APM 275, Oakland University, Winter 08
 Discrete Mathematics, APM 263, Oakland University, Fall 07
 Special Topics in Coding Theory, UMCS, Lublin, Poland, Spring 07
 Mathematics for Information and Technology, APM 163, Oakland Univ., Sp. 05
 Ordinary Differential Equations, Math 315, Univ. of Idaho, Fall 03, Sp. 05
 Linear Algebra, Math 330, Univ. of Idaho, Spring, Summer, Fall 04
 Abstract Algebra, Math 461, Univ. of Idaho, Fall 04
 Introduction to Cryptography, Math 435, Univ. of Idaho, Sp. 05
 Calculus I, II, UC Irvine
 Infinite Series and Complex Numbers, UC Irvine
 Elementary Linear Algebra, UC Irvine
 Linear Algebra I, II, UC Irvine
 Complex Analysis, UC Irvine

References upon request