Curriculum vitae

Angelo Sonnino

Work

Qualified as an associate professor for the area 01/A2 - Geometry and Algebra, Italian National Evaluation A.S.N. 2013.

Research associate of Geometry (subject code MAT/03) at the University of Basilicata since 1996.

He published the results of his research activity in international scientific journals and is inventor in an Italian patent.

Education

- In 2005 he obtained the academic title of Doctor of Philosophy (D.Phil.) in mathematics from the University of Sussex at Brighton UK. Title of the thesis: Ovals and arcs in finite projective planes, supervisor: Professor J.W.P. Hirschfeld.
- In the academic year 1990-1991 he obtained a scholarship from the Istituto Nazionale di Alta Matematica (Italian National Institute for Higher Mathematics) "Francesco Severi".
- In 1990 he obtained the Laurea (corresponding to both BA & MA Degrees) in Mathematics from the Sapienza University of Rome. Title of the thesis: "Curve algebriche e crittografia" (Algebraic Curves and Cryptography), supervisor: Professor M.J. de Resmini.

Research

His research interests are mainly in the area of discrete mathematics with particular regard to finite geometries. His research work has been focused on the following topics:

- arcs, ovals and hyperovals in finite geometries;
- cryptography;
- curves over finite fields;

- factorization of multigraphs;
- generalised affine spaces;
- coding theory.

Conferences

He presented his results in various international conferences and, in particular, he was invited to give talks at the following ones.

- Szeged (Hungary), 10–14 June 2013. Finite Geometry Conference and Workshop. Title of the talk: "Hughes planes and their collineations groups".
- Corfù (Greece), 30 May–4 June 2012. Fourth Pythagorean Conference. Title of the talk: "k-arcs for two–level secret–sharing schemes".
- Deerfield Beach, Florida (U.S.A.), 17–22 maggio 2009. Cryptology, Designs and Finite Groups 2009. Title of the talk: "LDPC codes arising from Singer cycles of proiettive spaces".
- Capri, NA (Italy), 7–10 June 2001. Discrete Mathematics and its Industrial Applications. Title of the talk: "Cryptosystems arising from hyperelliptic curves".
- Melfi, PZ (Italy), 19–23 June 2000. Advanced Special Functions and Integration Methods. Title of the talk: "Generalised affine spaces and their application to cryptography".
- Melfi, PZ (Italy), 9–12 maggio 1999. Advanced Special Functions and Applications. Title of the talk: "Resultants of polynomials, algebraic geometry and coding theory".

Invited talks at universities

- "Eötvös Loránd" University, Budapest, Hungary (5). Titles: "k-arcs in Benz planes", "Arcs in Möbius, Laguerre and Minkowski planes", "Recent results and open problems on arcs in circle geometries", "Projective k-arcs and 2-level secret-sharing schemes", "Arcs in Galois geometries and their applications".
- Szegedi Tudományegyetem, Seghedino, Hungary. Title: "Application of elliptic curves to cryptography".
- Milan Polytecnic, Milan, Italy (2). Titles: "Using algebraic curves in cryptography", "The geometry of cybersecurity and related problems".
- Second University of Naples, Caserta, Italy. Title: "The theory of arcs in Benz geometries".

- University of Brescia, Brescia, Italy (2). Titles: "New trends in cryptography", "Algebraic curves for cryptography: elliptic and hyperelliptic".
- University of Naples Federico II, Naples, Italy (2). Titles: "Algorithms in C++", "Problems connected with the implementation of an elliptic cryptosystem for telecommunications".
- University of Sussex, Brighton, UK. Title: "Arcs in Benz planes".

Organisation of conferences and schools

- Potenza, 5–9 September 2005. Summer School on Finite Geometries "Giuseppe Tallini" entitled *Graphs, Cryptology and Finite Geometries.*
- Potenza, 1–6 September 2003. Summer School on Finite Geometries "Giuseppe Tallini".
- Maratea (PZ), 2–8 June 2002. International conference Combinatorics 2002.
- Potenza, 8–18 June 1999. Socrates Intensive Programme "Finite Geometries and their Automorphisms".

Participation in financed research programs

- PRIN 2012 (Scientific Research Programme of Relevant National Interest) of the Italian Ministry of University and Education entitled "Geometric Structures, Combinatorics and their Applications".
- PRIN 2008 (Scientific Research Programme of Relevant National Interest) of the Italian Ministry of University and Education entitled "Galois geometries and incidence structures".
- Research project financed by the Hungarian Government TÁMOP-4.2.2.-08/1-2008-0008 (Társadalmi Megújulás Operatív Program - Operative programme for the social development) entitled "Data Collection and Information Processing Based on Sensor Networks".
- PRIN 2005 (Scientific Research Programme of Relevant National Interest) of the Italian Ministry of University and Education entitled "Geometric structures, combinatorics and their applications".
- Research project for industrial applications of finite geometry entitled "Development of a prototype for an HW/SW integrated system for secure multimedia transmission over both Internet and point-to-point lines, using the IPSEC and UMTS protocols, with a cryptographic component based on a new algorithm arising from functions derived from finite geometry". Company: Seleta Computer S.r.l. (2004–2006).

- PRIN 2003 (Scientific Research Programme of Relevant National Interest) of the Italian Ministry of University and Education entitled "Geometric structures and their applications".

- PRIN 2001 (Scientific Research Programme of Relevant National Interest) of the Italian Ministry of University and Education entitled "Geometric structures, combinatorics and their applications".

- Program for the scientific and technologic cooperation between Italy and Hungary of the Italian Ministry of Foreign Affairs entitled "Geometric structures and their applications" (2000–2003).

- Research project for industrial applications of finite geometry entitled "Development of a prototype for a hardware module dedicated to the security of data transmission over the Internet concerning financial transactions and administrative tasks according to the current laws". Participating organizations: Sinter & Net S.p.A., Department of Mathematics of the University of Basilicata and Seleta Computer S.r.l. (2002).

- PRIN 1999 (Scientific Research Programme of Relevant National Interest) of the Italian Ministry of University and Education entitled "Geometric structures and their applications".

- POP-FESR Programme (Research, development and innovation) of the Basilicata Regional Council, II triennium 19941999 entitled "Project and development of a crypto system for telecommunications". Participating organizations: Basilicata Regional Council, Department of Mathematics of the University of Basilicata and Seleta Computer S.r.l.

- PRIN 1997 (Scientific Research Programme of Relevant National Interest) of the Italian Ministry of University and Education entitled "Geometric structures and their automorphism groups".

- Program for the scientific and technologic cooperation between Italy and Hungary of the Italian Ministry of Foreign Affairs entitled "Algebraic and geometric structures and their applications". (1996–1998).

Teaching

He carried out his teaching activity mostly at the University of Basilicata where, in particular, he gave the following courses.

- School of Engineering (formerly Faculty of Engineering): Geometry; Calculus I; Calculus II; Applied mathematics.

- Department of Mathematics, Computer Science and Economics (formerly Faculty of Sciences): Geometry I; Coding theory; Geometry of communication systems: coding theory and cryptography.

- Department of Humanities (formerly Faculty of Literature): Geometry for primary school teachers.

He also gave the following advanced courses abroad within the Erasmus Teaching Staff Mobility programme.

- Szegedi Tudományegyetem, Szeged, Hungary (6): "Ovals and arcs in finite projective planes" (2); "Geometric aspects of error correcting codes" (2); "Finite geometry with focus on its applications to coding theory and cryptography"; "k-arcs and two-level secret-sharing schemes".
- "Eötvös Loránd" University, Budapest, Hungary: "Algebraic curves and cryptography".

Other

He was referee for the following scientific journals:

- Discrete Applied Mathematics, ISSN: 0166-218X;
- Discrete Mathematics, ISSN: 0012-365X;
- Electronic Journal of Combinatorics, ISSN: 1077-8926;
- Innovations in Incidence Geometry, ISSN: 1781-6475;
- Journal of Algebraic Combinatorics, ISSN: 0925-9899 (print), 1572-9192 (electronic);
- Journal of Combinatorial Designs, ISSN: 1063-8539;
- Journal of Geometry, ISSN: 0047-2468;
- Journal of Mathematical Cryptology, ISSN: 1862-2976 (print), 1862-2984 (electronic);
- Radovi Matematički, ISSN: 0352-6100.

He is member of the following associations:

- G.N.S.A.G.A. - Gruppo Nazionale per le Strutture Algebriche, Geometriche e le Loro Applicazioni dellINdAM - Istituto Nazionale di Alta Matematica "Francesco Severi" (Italian National Research Group on Algebraic and Geometric Structures and Their Applications of INdAM - Italian National Institute for Higher Mathematics Francesco Severi);
- Unione Matematica Italiana (Italian Mathematical Society).

He uses the MAGMA and GAP for computations in algebra, number theory, algebraic geometry and algebraic combinatorics. He also knows the MATHEMATICA package and the programming languages C and C++.

He is fluent in the following languages:

- Italian (native speaker);
- English.

He can also read mathematics in the following languages:

- French;
- Spanish.

Publications

[1] On linear codes admitting large automorphism groups (con N. Pace), *Des. Codes Cryptogr.* (2016), DOI: 10.1007/s10623-016-0207-6.

[2] Existence of canonically inherited arcs in Moulton planes of odd order, *Finite Fields Appl.* **33** (2015), 187–197.

[3] A remark on Hamming codes (con A. Cossidente e C. Nolè), *Bull. Inst. Combin. Appl.* **74** (2015), 47–52.

[4] Transitive PSL$(2, 7)$-invariant 42-arcs in 3-dimensional projective spaces, *Des. Codes Cryptogr.* **72** (2014), No. 2, 455–463.

[5] On graphs and codes associated to the sporadic simple groups HS and M_{22} (con A. Cossidente), *Australas. J. Combin.* **60** (2014), No. 2, 208–216.

[6] Old and recent results on finite Bolyai-Lobachevskii planes (con G. Korchmáros), *Mathematica* **56 (79)** (2014), No. 1, 59–73.

[7] Cap codes arising from duality (con A. Cossidente e C. Nolè), *Bull. Inst. Combin. Appl.* **67** (2013), 33–42.

[8] Doubly transitive parabolic ovals in affine planes of even order $n \leq 64$ (con G. Korchmáros), *Ars Combin.* **105** (2012), 419–433.

[9] Projective k-arcs and 2-level secret-sharing schemes (con G. Korchmáros e V. Lanzone), *Des. Codes Cryptogr.* **64** (2012), No. 1–2, 3–15.

[10] Finite Bolyai-Lobachevskii planes (con G. Korchmáros), *Acta Math. Hungar.* **134** (2012), No. 4, 405–415.

[11] Linear codes arising from the Gale transform of distinguished subsets of some projective spaces (con A. Cossidente), *Discrete Math.* **312** (2012), 647–651.

[12] Finite geometry and the Gale transform (con A. Cossidente), *Discrete Math.* **310** (2010), 3206–3210.

[13] Some recent results in finite geometry and coding theory arising from the Gale transform (con A. Cossidente), *Rend. Mat. Appl. (7)* **30** (2010), 67–76.

[14] On arcs sharing the maximum number of points with ovals in cyclic affine planes of odd order (con G. Korchmáros), *J. Combin. Des.* **18** (2010), No. 1, 25–47.

[15] LDPC codes from Singer cycles (con L. Giuzzi), *Discrete Appl. Math.* **157** (2009), 1723–1728.

[16] A geometric construction of a $[110, 5, 90]_9$-linear code admitting the Mathieu group M_{11} (con A. Cossidente), *IEEE Trans. Inform. Theory* **54** (2008), No. 11, 5251–5252.

[17] S-spaces from free extensions, *Contrib. Discrete Math.* **3** (2008), No. 1, 58–62.

[18] Brevetto n. 0001379714 (domanda n. TO2007A00400), Ufficio Italiano Brevetti e Marchi. *Perfezionamenti nella crittografia a chiave pubblica basata su curve ellittiche* (con L. Giuzzi e G. Korchmáros). Seleta, Società Elettronica Tecnologie Avanzate S.r.l. 2007.

[19] Ovals in a plane coordinatised by a regular nearfield of dimension 2 over its centre, *J. Geom.* **82** (2005), 188–194.

[20] Transitive hyperovals in finite projective planes, *Australas. J Combin.* **33** (2005), 335–347.

[21] Hyperbolic ovals in finite planes (con G. Korchmáros), *Des. Codes Cryptogr.* **32** (2004), No. 1–3, 239–249.

[22] *Ovals and arcs in finite projective planes,* tesi Ph.D., University of Sussex, Brighton, Regno Unito, 2004, British Library No. 013182113.

[23] Symmetric configurations arising from mixed partitions of projective geometries (con A. Aguglia ed A. Cossidente), *Int. J. Pure Appl. Math.* **7** (2003), No. 3, 369– 379.

[24] Two methods for constructing S-spaces, *Atti Sem. Mat. Fis. Univ. Modena* **51** (2003), 65–71.

[25] Complete arcs arising from conics (con G. Korchmáros), *Discrete Math.* **267** (2003), No. 1–3, 181–187.

[26] Jacobians of hyperelliptic curves for cryptography, *Pure Math. Appl.* **13** (2002), No. 3, 399–415.

[27] Complete arcs in inversive planes over prime fields (con É. Hadnagy), *Discrete Math.* **255** (2002), No. 1–3, 181–188.

[28] Some results on generalised affine spaces and their applications, *Advanced Special Functions and Integration Methods (Melfi, 2000),* Proc. Melfi Sch. Adv. Top. Math. Phys., 2, Aracne, Rome, 2001, pp. 339–350.

[29] One-factorizations of complete multigraphs arising from maximal $(k;n)$-arcs in $\mathrm{PG}(2,2^h)$, *Discrete Math.* **231** (2001), No. 2-3, 447–451.

[30] 1-factorizations of complete multigraphs arising from finite geometry (con G. Korchmáros e A. Siciliano), *J. Combin. Theory Ser. A* **93** (2001), No. 2, 385–390.

[31] Coding theory and algebraic geometry (con G. Korchmáros), *Advanced Special Functions and Applications (Melfi, 1999),* Proc. Melfi Sch. Adv. Top. Math. Phys., 1, Aracne, Rome, 2000, pp. 325–336.

[32] Cryptosystems based on latin rectangles and generalised affine spaces, *Rad. Mat.* **9** (1999), No. 2, 177–186.

[33] Large k-arcs in inversive planes of odd order, *J. Geom.* **66** (1999), No. 1-2, 187–191.

[34] Linear collineation groups preserving an arc in a Möbius plane, *Discrete Math.* **197/198** (1999), 749–757.