Curriculum vitae

Angelo Sonnino

Lavoro

Abilitazione Scientifica Nazionale come professore associato per il settore concorsuale 01/A2 - Geometria e Algebra, A.S.N. 2013.

Ricercatore per il settore scientifico disciplinare MAT/03 (Geometria) presso l'Università della Basilicata dal 1996.

Ha pubblicato i risultati della propria ricerca su riviste scientifiche internazionali ed è inventore in un brevetto industriale.

Studi

- Nel 2005 ha ottenuto il dottorato di ricerca (D.Phil.) in matematica presso la University of Sussex in Brighton (Regno Unito). Titolo della tesi: "Ovals and arcs in finite projective planes", supervisore: prof. J.W.P. Hirschfeld.
- Nell'Anno Accademico 1990-1991 ha usufruito di una borsa di studio presso l'Istituto Nazionale di Alta Matematica "Francesco Severi".
- Nel 1990 ha ottenuto la Laurea in Matematica presso la Sapienza Università di Roma. Titolo della tesi: "Curve algebriche e crittografia", relatrice: prof.ssa M.J. de Resmini.

Ricerca

La parte essenziale del suo lavoro scientifico si colloca nell'ambito della matematica discreta ed in particolare delle geometrie combinatorie. Nella sua attività di ricerca si è occupato dei seguenti argomenti:

- archi, ovali ed iperovali nelle geometrie finite;
- crittografia;
- curve sopra campi finiti;
- fattorizzazione di multigrafi;
- spazi affini generalizzati;

- teoria dei codici.

Convegni

Ha presentato i risultati della propria ricerca a numerosi convegni internazionali, ed in particolare è stato invitato ai seguenti convegni.

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

Conferenze su invito presso università

- "Eötvös Loránd" University, Budapest, Ungheria (5). Titoli: "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, Szeged, Ungheria. Titolo: "Application of elliptic curves to cryptography".
- Politecnico di Milano (2). Titoli: "Uso delle curve algebriche in crittografia", "Geometria della sicurezza informatica e problemi connessi".
- Seconda Università di Napoli, Caserta. Titolo: "La teoria degli archi nelle geometrie di Benz".
- Università degli Studi di Brescia (2). Titoli: "Nuove tendenze in crittografia", "Curve algebriche per la crittografia: ellittiche ed iperellittiche".

- Università degli Studi di Napoli "Federico II" (2). Titoli: "Algoritmi in C++", "Problemi di implementazione di un criptosistema ellittico per telecomunicazioni".
- University of Sussex, Brighton, Regno Unito. Titolo: "Arcs in Benz planes".

Organizzazione convegni e scuole

- Potenza, 8–18 giugno 1999. Scuola Estiva di Geometrie Combinatorie—Socrates Intensive Programme "Finite Geometries and their Automorphisms".
- Maratea (PZ), 2–8 giugno 2002. Convegno internazionale Combinatorics 2002.
- Potenza, 1–6 settembre 2003. Scuola Estiva di Geometrie Combinatorie "Giuseppe Tallini".
- Potenza, 5–9 settembre 2005. Scuola Estiva di Geometrie Combinatorie "Giuseppe Tallini" dal titolo: *Graphs, Cryptology and Finite Geometries.*

Partecipazione a progetti di ricerca finanziati

- PRIN 2012 (Programma di Ricerca Scientifica di Rilevante Interesse Nazionale) dal titolo "Strutture Geometriche, Combinatoria e loro Applicazioni".
- PRIN 2008 (Programma di Ricerca Scientifica di Rilevante Interesse Nazionale) dal titolo "Geometrie di Galois e strutture di incidenza".
- Progetto di ricerca finanziato dal Governo Ungherese TÁMOP-4.2.2.-08/1-2008-0008 (Társadalmi Megújulás Operatív Program - Programma operativo per il rinnovamento sociale) dal titolo "Data Collection and Information Processing Based on Sensor Networks".
- PRIN 2005 (Programma di Ricerca Scientifica di Rilevante Interesse Nazionale) dal titolo "Strutture geometriche, combinatoria e loro applicazioni".
- Progetto di ricerca per applicazioni industriali della geometria combinatoria dal titolo "Ricerca e sviluppo di un sistema prototipale integrato HW/SW dedicato alle trasmissioni multimediali crittografate, in ambiente Internet e su linee dedicate punto-punto, basato su protocollo IPSEC ed UMTS, utilizzando come elemento crittografico un algoritmo innovativo implementato con funzioni di geometria combinatoria". Azienda finanziatrice: Seleta Computer S.r.l. (2004–2006).
- PRIN 2003 (Programma di Ricerca Scientifica di Rilevante Interesse Nazionale) dal titolo "Strutture geometriche e loro applicazioni".

- PRIN 2001 (Programma di Ricerca Scientifica di Rilevante Interesse Nazionale) dal titolo “Strutture geometriche, combinatorica e loro applicazioni”.
- Programma per la cooperazione scientifica e tecnologica italo–ungherese del M.A.E. (Ministero degli Affari Esteri) dal titolo “Strutture geometriche e loro applicazioni” (2000–2003).
- Progetto di ricerca per applicazioni industriali della geometria combinatoria dal titolo “Analisi, progettazione e prototipazione di un modulo hardware dedicato alla protezione delle trasmissioni di dati veicolati su rete Internet per transazioni economiche e gestioni di processi in ottemperanza alle vigenti normative”. Enti partecipanti: Sinter & Net S.p.A., Dipartimento di Matematica dell’Università degli Studi della Basilicata e Seleta Computer S.r.l. (2002).
- PRIN 1999 (Programma di Ricerca Scientifica di Rilevante Interesse Nazionale) dal titolo “Strutture geometriche e loro applicazioni”.
- Programma POP-FESR (Ricerca, sviluppo e innovazione) della Regione Basilicata, II triennio 1994–1999, dal titolo “Progetto e realizzazione di un criptosistema per telecomunicazioni”. Enti partecipanti: Regione Basilicata, Dipartimento di Matematica dell’Università degli Studi della Basilicata, Seleta Computer S.r.l.
- PRIN 1997 (Programma di Ricerca Scientifica di Rilevante Interesse Nazionale) dal titolo “Strutture geometriche e loro gruppi di automorfismi”.
- Programma per la cooperazione scientifica e tecnolologica italo-ungherese del M.A.E. (Ministero degli Affari Esteri) dal titolo “Strutture algebriche, geometriche e loro applicazioni”. (1996–1998).

Didattica

La sua attività didattica si è svolta prevalentemente presso l’Università degli Studi della Basilicataove, in particolare, ha tenuto i seguenti corsi.

- Scuola di Ingegneria (già Facoltà di Ingegneria): Geometria; Analisi matematica I; Analisi matematica II; Matematica applicata.
- Dipartimento di Matematica, Informatica ed Economia (già Facoltà di Scienze MM.FF.NN.): Geometria I; Teoria dei codici; Geometria dei sistemi di comunicazione: teoria dei codici e crittografia.
- Dipartimento di Scienze Umane (già Facoltà di Lettere e Filosofia): Geometria per il corso di laurea in Scienze della Formazione.

Ha inoltre tenuto i seguenti corsi avanzati all’estero nell’ambito del progetto Erasmus Teaching Staff Mobility.

- Szegedi Tudományegyetem, Szeged, Ungheria (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, Ungheria: "Algebraic curves and cryptography".

Altre attività e competenze

È stato recensore di articoli scientifici per le seguenti riviste:

- 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.

È membro delle seguenti associazioni:

- G.N.S.A.G.A. (INdAM) Gruppo Nazionale per le Strutture Algebriche, Geometriche e le loro Applicazioni;
- Unione Matematica Italiana.

Usa correntemente i pacchetti MAGMA e GAP per il calcolo scientifico in algebra, teoria dei numeri, geometria algebrica e combinatoria algebrica. Conosce inoltre il pacchetto di calcolo MATHEMATICA ed i linguaggi di programmazione C e C++.

Parla correntemente le seguenti lingue:

- Italiano (madrelingua);
- Inglese.

Legge testi di matematica anche nelle seguenti lingue:

- Francese;
- Spagnolo.

Pubblicazioni

[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.