

# Curriculum vitae con elenco delle pubblicazioni

**Angelo Sonnino**

7 luglio 2020

# Angelo Sonnino

Email: [angelo.sonnino@unibas.it](mailto:angelo.sonnino@unibas.it)  
Web: [web.unibas.it/sonnino](http://web.unibas.it/sonnino)  
Indirizzo: Dipartimento di Matematica, Informatica  
ed Economia  
Università degli Studi della Basilicata  
Via dell'Ateneo Lucano, 10  
85100 Potenza - PZ

## Lavoro

- Abilitazione Scientifica Nazionale da professore associato (A.S.N. 2013) per il settore concorsuale 01/A2 - Geometria e Algebra.
- Dal 1996 ricercatore presso il Dipartimento di Matematica, Informatica ed Economia dell'Università degli Studi della Basilicata, Potenza, per il settore scientifico-disciplinare MAT/03 - Geometria.
- Nel 1992 ha conseguito l'abilitazione all'insegnamento della matematica per la Scuola Media Superiore, classe A063, con il concorso istituito con D.M. del 23 marzo 1990.

## Studi

- 2005. D.Phil. (dottorato di ricerca) in Matematica conseguito presso la University of Sussex di Brighton, Regno Unito, con una tesi dal titolo: "Ovals and arcs in finite projective planes". Relatore 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" (INdAM).
- 1990. Laurea in Matematica conseguita presso la Sapienza Università di Roma con una tesi dal titolo: "Curve Algebriche e Crittografia". Relatrice prof.ssa M. J. de Resmini.
- 1973. Diploma di Maturità Classica conseguito presso il Liceo Classico Statale "Ennio Quirino Visconti" di Roma.

## Aree di ricerca

**N.B.** Per ogni settore disciplinare viene riportata la classificazione AMS.

**05C70** fattorizzazioni di multigrafi completi e loro legami con le geometrie finite;

**11G20** curve su campi finiti;

**20B25** gruppi di automorfismi di strutture combinatorie;

- 51A15** strutture di incidenza con parallelismo che generalizzano la nozione di spazio affine, S-spazi;
- 51E20** configurazioni tattiche e loro rappresentazione geometrica;
- 51E21** teoria degli archi nei piani proiettivi, negli spazi proiettivi e nelle geometrie di Benz;
- 94A60** crittografia;
- 94B27** teoria dei codici.

## Publicazioni

- [1] N. Pace, A. Sonnino. On the existence of PD-sets: Algorithms arising from automorphism groups of codes. *Adv. Math. Commun.* (online first 2020), doi: 10.3934/amc.2020065.
- [2] S. Caputo, G. Korchmáros, A. Sonnino. Multilevel secret sharing schemes arising from the normal rational curve. *Discrete Appl. Math.* **284** (2020), 158–165.
- [3] N. Pace, A. Sonnino. One-factorisations of complete graphs constructed in Desarguesian planes of certain odd square orders, *Electron. J. Combin.* **27** (2020), No. 1, Paper 3.54, 13 pp.
- [4] Gy. Kiss, N. Pace, A. Sonnino. On circular-linear one-factorizations of the complete graph  $K_n$ , *Discrete Math.* **342** (2019), No. 12, Art. 111622.
- [5] N. Pace, A. Sonnino. One-factorisations of complete graphs arising from hyperbolae in the Desarguesian affine plane, *J. Geom.* **110** (2019), No. 1, Art 15.
- [6] G. Korchmáros, N. Pace, A. Sonnino. One-factorisations of complete graphs arising from ovals in finite planes, *J. Combin. Theory Ser. A* **160** (2018), 62–83.
- [7] G. Korchmáros, A. Sonnino, T. Szőnyi. Inherited unitals in Moulton planes *Ars Math. Contemp.* **14** (2018), No. 2, 251–265.
- [8] N. Pace, A. Sonnino. On linear codes admitting large automorphism groups, *Des. Codes Cryptogr.* **83** (2017), nN. 1, 115–143.
- [9] A. Sonnino. Existence of canonically inherited arcs in Moulton planes of odd order, *Finite Fields Appl.* **33** (2015), 187–197.
- [10] A. Cossidente C. Nolè, A. Sonnino. A remark on Hamming codes, *Bull. Inst. Combin. Appl.* **74** (2015), 47–52.
- [11] A. Sonnino. Transitive  $\text{PSL}(2,7)$ -invariant 42-arcs in 3-dimensional projective spaces, *Des. Codes Cryptogr.* **72** (2014), No. 2, 455–463.
- [12] A. Cossidente, A. Sonnino. On graphs and codes associated to the sporadic simple groups HS and  $M_{22}$ , *Australas. J. Combin.* **60** (2014), No. 2, 208–216.

- [13] G. Korchmáros, A. Sonnino. Old and recent results on finite Bolyai-Lobachevskii planes, *Mathematica* **56 (79)** (2014), No. 1, 59–73.
- [14] A. Cossidente C. Nolè, A. Sonnino. Cap codes arising from duality, *Bull. Inst. Combin. Appl.* **67** (2013), 33–42.
- [15] G. Korchmáros, A. Sonnino. Doubly transitive parabolic ovals in affine planes of even order  $n \leq 64$ , *Ars Combin.* **105** (2012), 419–433.
- [16] G. Korchmáros, V. Lanzone, A. Sonnino. Projective  $k$ -arcs and 2-level secret-sharing schemes, *Des. Codes Cryptogr.* **64** (2012), No. 1–2, 3–15.
- [17] G. Korchmáros, A. Sonnino. Finite Bolyai-Lobachevskii planes, *Acta Math. Hungar.* **134** (2012), No. 4, 405–415.
- [18] A. Cossidente, A. Sonnino. Linear codes arising from the Gale transform of distinguished subsets of some projective spaces, *Discrete Math.* **312** (2012), 647–651.
- [19] A. Cossidente, A. Sonnino. Finite geometry and the Gale transform, *Discrete Math.* **310** (2010), 3206–3210.
- [20] G. Korchmáros, A. Sonnino. On arcs sharing the maximum number of points with ovals in cyclic affine planes of odd order, *J. Combin. Des.* **18** (2010), No. 1, 25–47.
- [21] A. Cossidente, A. Sonnino. Some recent results in finite geometry and coding theory arising from the Gale transform, *Rend. Mat. Appl. (7)* **30** (2010), 67–76.
- [22] L. Giuzzi, A. Sonnino. LDPC codes from Singer cycles, *Discrete Appl. Math.* **157** (2009), 1723–1728.
- [23] A. Cossidente, A. Sonnino. A geometric construction of a  $[110, 5, 90]_9$ -linear code admitting the Mathieu group  $M_{11}$ , *IEEE Trans. Inform. Theory* **54** (2008), No. 11, 5251–5252.
- [24] A. Sonnino. S-spaces from free extensions, *Contrib. Discrete Math.* **3** (2008), No. 1, 58–62.
- [25] A. Sonnino, Ovals in a plane coordinatised by a regular nearfield of dimension 2 over its centre, *J. Geom.* **82** (2005), 188–194.
- [26] A. Sonnino. Transitive hyperovals in finite projective planes, *Australas. J. Combin.* **33** (2005), 335–347.
- [27] G. Korchmáros, A. Sonnino. Hyperbolic ovals in finite planes, *Des. Codes Cryptogr.* **32** (2004), No. 1–3, 239–249.
- [28] A. Sonnino. Ovals and arcs in finite projective planes, Ph.D. thesis, University of Sussex, Brighton, Regno Unito, 2004, British Library No. 013182113.
- [29] G. Korchmáros, A. Sonnino. Complete arcs arising from conics, *Discrete Math.* **267** (2003), No. 1–3, 181–187.

- [30] A. Aguglia, A. Cossidente, A. Sonnino. Symmetric configurations arising from mixed partitions of projective geometries, *Int. J. Pure Appl. Math.* **7** (2003), No. 3, 369–379.
- [31] A. Sonnino. Two methods for constructing S-spaces, *Atti Sem. Mat. Fis. Univ. Modena* **51** (2003), 65–71.
- [32] É. Hadnagy, A. Sonnino. Complete arcs in inversive planes over prime fields, *Discrete Math.* **255** (2002), No. 1–3, 181–188.
- [33] A. Sonnino. Jacobians of hyperelliptic curves for cryptography, *Pure Math. Appl.* **13** (2002), No. 3, 399–415.
- [34] G. Korchmáros, A. Siciliano, A. Sonnino. 1-factorizations of complete multigraphs arising from finite geometry, *J. Combin. Theory Ser. A* **93** (2001), No. 2, 385–390.
- [35] A. Sonnino. One-factorizations of complete multigraphs arising from maximal  $(k; n)$ -arcs in  $PG(2, 2^h)$ , *Discrete Math.* **231** (2001), No. 2-3, 447–451.
- [36] A. Sonnino. 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.
- [37] G. Korchmáros, A. Sonnino. Coding theory and algebraic geometry, *Advanced Special Functions and Applications (Melfi, 1999)*, Proc. Melfi Sch. Adv. Top. Math. Phys., 1, Aracne, Rome, 2000, pp. 325–336.
- [38] A. Sonnino. Linear collineation groups preserving an arc in a Möbius plane, *Discrete Math.* **197/198** (1999), 749–757.
- [39] A. Sonnino. Large  $k$ -arcs in inversive planes of odd order, *J. Geom.* **66** (1999), No. 1-2, 187–191.
- [40] A. Sonnino. Cryptosystems based on latin rectangles and generalised affine spaces, *Rad. Mat.* **9** (1999), No. 2, 177–186.

## Brevetto

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

## Partecipazione a progetti di ricerca finanziati

- PRIN (Programma di Ricerca Scientifica di Rilevante Interesse Nazionale) 2012 dal titolo “Strutture Geometriche, Combinatoria e loro Applicazioni” (36 mesi).
- PRIN (Programma di Ricerca Scientifica di Rilevante Interesse Nazionale) 2008 dal titolo “Geometrie di Galois e Strutture di Incidenza” (24 mesi).

- PRIN (Programma di Ricerca Scientifica di Rilevante Interesse Nazionale) 2005 dal titolo “Strutture Geometriche, Combinatoria e loro Applicazioni” (24 mesi).
- 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 Dedicare 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) (36 mesi).
- PRIN (Programma di Ricerca Scientifica di Rilevante Interesse Nazionale) 2003 dal titolo “Strutture Geometriche e loro Applicazioni” (24 mesi).
- PRIN (Programma di Ricerca Scientifica di Rilevante Interesse Nazionale) 2001 dal titolo “Strutture Geometriche, Combinatoria e loro Applicazioni” (24 mesi).
- Programma per la cooperazione scientifica e tecnologica italo–ungherese del M.A.E. (Ministero degli Affari Esteri) Titolo del progetto: “Strutture Geometriche e loro Applicazioni” (2000–2003) (48 mesi).
- 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) (12 mesi).
- PRIN (Programma di Ricerca Scientifica di Rilevante Interesse Nazionale) 1999 dal titolo “Strutture geometriche e loro applicazioni” (24 mesi).
- Programma POP-FESR (Ricerca, Sviluppo e Innovazione) della Regione Basilicata, II triennio 1994–1999, dal titolo: “Progetto e Realizzazione di un Criosistema per Telecomunicazioni”. Enti partecipanti: Regione Basilicata, Dipartimento di Matematica dell’Università degli Studi della Basilicata, Seleta Computer S.r.l. (36 mesi).
- PRIN (Programma di Ricerca Scientifica di Rilevante Interesse Nazionale) 1997 dal titolo “Strutture Geometriche e loro Gruppi di Automorfismi” (24 mesi).
- Programma per la cooperazione scientifica e tecnologica italo-ungherese del M.A.E. (Ministero degli Affari Esteri) dal titolo “Strutture Algebriche, Geometriche e loro Applicazioni”. (1996–1998) (36 mesi).

## Affiliazioni

- Unione Matematica Italiana;
- Associazione nazionale di crittografia “De Componendis Cifris”;

- Gruppo Nazionale per le Strutture Algebriche, Geometriche e le loro Applicazioni (GNSAGA) dell'Istituto Nazionale di Alta Matematica "F. Severi" (INdAM).

## Dottorato di Ricerca

- Membro del Collegio dei Docenti Del Dottorato di Ricerca in Matematica e Informatica dell'Università del Salento [DOT1312455] dal XXXV ciclo (2019/2020).
- Membro del Collegio dei Docenti del Dottorato di Ricerca Internazionale in Matematica "János Bolyai" (in collaborazione fra l'Università degli Studi della Basilicata, Potenza e la Szegedi Tudományegyetem, Szeged, Ungheria) dal XXIII ciclo (2007/2008) al XXVIII ciclo (2012/2013).

## Attività didattica

### Corso per il Dottorato di Ricerca Internazionale in Matematica "János Bolyai"

- crittografia 1 nell'anno accademico 2007/2008.

### Corsi presso il Dipartimento di Matematica, Informatica ed Economia - DiMIE (già Facoltà di Scienze MM.FF.NN.) dell'Università degli Studi della Basilicata

- teoria dei codici per i corsi di laurea in matematica dall'anno accademico 2010/2011;
- statistica (codocenza) nell'anno accademico 2015/2016;
- geometria dei sistemi di comunicazione: teoria dei codici e crittografia per il corso di laurea in matematica, mutuato come teoria dei codici per il corso di laurea specialistica in informatica, nell'anno accademico 2009/2010;
- geometria I per il corso di laurea in matematica nell'anno accademico 2008/2009.

### Corsi presso Dipartimento delle Culture Europee e del Mediterraneo: architettura, ambiente, patrimoni culturali - DiCEM (già Facoltà di Architettura) dell'Università degli Studi della Basilicata

- geometria per il corso di laurea magistrale in architettura dall'anno accademico 2008/2009.

### Corsi presso la Scuola di Ingegneria - SI-UniBas (già Facoltà di Ingegneria) dell'Università degli Studi della Basilicata

- geometria per tutti i corsi di laurea dall'anno accademico 2007/2008 al 2013/2014;
- integrazione e calcolo differenziale in più variabili/analisi matematica II per tutti i corsi di laurea dall'anno accademico 1999/2000 al 2001/2002 e dal 2005/2006 al 2006/2007;

- calcolo differenziale in una variabile/analisi matematica I per tutti i corsi di laurea dall'anno accademico 2002/2003 al 2004/2005.

**Corsi presso il Dipartimento di Scienze Umane - DiSU (già Facoltà di Lettere e Filosofia) dell'Università degli Studi della Basilicata**

- geometria per il corso di laurea in scienze della formazione primaria negli anni accademici 2006/2007 e 2007/2008.

**Erasmus Teaching Staff Mobility (STA)**

- Szegedi Tudományegyetem di Szeged (Ungheria): 10 ore di docenza dal 2 al 7 settembre 2019 nell'ambito del corso istituzionale intitolato "Finite Geometries and Codes", anno accademico 2018/2019. Titolo del ciclo di lezioni: *Error correcting codes and geometries over finite fields.*
- Szegedi Tudományegyetem di Szeged (Ungheria): 10 ore di docenza dal 4 all'8 settembre 2018 nell'ambito del corso istituzionale intitolato "Finite Geometries and Codes", anno accademico 2017/2018. Titolo del ciclo di lezioni: *Introduction to the theory of error correcting codes.*
- Szegedi Tudományegyetem di Szeged (Ungheria): 10 ore di docenza dall'8 al 13 settembre 2017 nell'ambito del corso istituzionale intitolato "Geometries and Codes", anno accademico 2016/2017. Titolo del ciclo di lezioni: *Introduction to the theory of error correcting codes.*
- Szegedi Tudományegyetem di Szeged (Ungheria): 16 ore di docenza dal 3 al 12 maggio 2016 nell'ambito del corso istituzionale di geometrie finite, anno accademico 2015/2016. Titolo del ciclo di lezioni: *Ovals and arcs in finite projective planes.*
- Szegedi Tudományegyetem di Szeged (Ungheria): 8 ore di docenza dal 5 al 15 aprile 2014 nell'ambito del corso istituzionale di geometrie finite, anno accademico 2013/2014. Titolo del ciclo di lezioni: *Ovals and arcs in finite projective planes.*
- Szegedi Tudományegyetem di Szeged (Ungheria): 8 ore di docenza dal 7 al 13 aprile 2013 nell'ambito del corso istituzionale di geometrie finite, anno accademico 2012/2013. Titolo del ciclo di lezioni: *Geometric aspects of error correcting codes.*
- Szegedi Tudományegyetem di Szeged (Ungheria): 8 ore di docenza dal 16 al 23 aprile 2012 nell'ambito del corso istituzionale di geometrie finite, anno accademico 2011/2012. Titolo del ciclo di lezioni: *Geometric aspects of error correcting codes.*
- Szegedi Tudományegyetem di Szeged (Ungheria): 8 ore di docenza dal 2 al 12 settembre 2011 nell'ambito del corso istituzionale di geometrie finite, anno accademico 2010/2011. Titolo del ciclo di lezioni: *Finite geometry with focus on its applications to coding theory and cryptography.*
- Szegedi Tudományegyetem di Szeged (Ungheria): 8 ore di docenza dal 26 aprile al 1 maggio 2010 nell'ambito del corso istituzionale di geometrie finite, anno accademico 2009/2010. Titolo del ciclo di lezioni: *k-arcs and two-level secret sharing systems.*

- “Eötvös Loránd” Tudományegyetem di Budapest (Ungheria): 10 ore di docenza dal 17 al 23 marzo 2002 nell’ambito del corso istituzionale di geometria IV, anno accademico 2001/2002. Titolo del ciclo di lezioni: *Algebraic curves and cryptography*.

## Convegni, corsi e soggiorni di ricerca

### Organizzazione

Potenza, 21 settembre 2018. Workshop *GK70 - A Day of Geometry in Honour of Gábor Korchmáros*.

Maratea (PZ), 29 maggio–4 giugno 2016. Convegno internazionale Combinatorics 2016 (anche nel Comitato Scientifico).

Potenza, 5–9 settembre 2005. Scuola Estiva di Geometrie Combinatorie “Giuseppe Tallini” dal titolo: *Graphs, Cryptology and Finite Geometries*.

Potenza, 1–6 settembre 2003. Scuola Estiva di Geometrie Combinatorie “Giuseppe Tallini”.

Maratea (PZ), 2–8 giugno 2002. Convegno internazionale Combinatorics 2002 (anche nel Comitato Scientifico).

Potenza, 8–18 giugno 1999. Scuola Estiva di Geometrie Combinatorie—Socrates Intensive Programme “Finite Geometries and their Automorphisms”.

### Partecipazione

Più di 80 fra convegni nazionali e internazionali, soggiorni di ricerca e conferenze su invito.