Curriculum vitae

Luca Giuzzi

Thursday 11th July, 2024

1 Personal details

Surname:	Giuzzi
Name:	Luca
Title:	Dr. (DPhil, Sussex)
Role:	Associate Professor of Geometry
Date of Birth:	30 September 1973
Citizenship:	Italian
Known languages:	Italian (mother-tongue), English (fluent).
Telephone (BS):	+39 030 3715739
Fax:	+39 030 3715745
E-mail:	luca.giuzzi@unibs.it
Web page:	`http://luca-giuzzi.unibs.it`
ORCID:	0000-0003-3975-7281
ResearcherID:	F-4066-2010
Address (work):	DICATAM Section of Mathematics Facoltà di Ingegneria Università degli studi di Brescia via Branze 43 25123 Brescia ITALY
Address (home):	via Cesare Battisti 42 25018 Montichiari (BS) ITALY

2 Studies

1. *Laurea in matematica* (degree in mathematics) with a score of 110 *cum laude*/110, Università Cattolica del Sacro Cuore; thesis "Gruppi di Frobenius e strutture geometriche associate" under the supervision of Prof. Silvia Pianta, 1996.
2. DPhil in Mathematics, University of Sussex; thesis "Hermitian varieties over finite field" under the supervision of Prof. James Hirschfeld, 2001.

3 Employment history

1. 1992-1996: Undergraduate student at Università Cattolica del Sacro Cuore.
2. 1996-1997: Unix system administrator at Università Cattolica.
3. 1997-2000: DPhil student at University of Sussex.
4. 2000-2004: research fellow at Università degli studi di Brescia.
5. 2002-2003: work on "Development of a cryptosystem based on elliptic or hyperelliptic curves" (POP 342) in collaboration with Università della Basilicata.

6. 2004-April 2008: research associate in Geometry at Politecnico di Bari.
7. May 2008-2018: research associate in Geometry at Università degli Studi di Brescia.
8. June 2018-now: associate professor of Geometry at Università degli Studi di Brescia.

4 Habilitations

Luca Giuzzi has been qualified (habilitated) by the italian MUR to the role of

1. *associate professor in Geometry* on March 28, 2017;
2. *full professor in Geometry* on July 8, 2024.

5 Refereeing activity

Luca Giuzzi has been acting as *referee* for several international journals, including *Annals of Combinatorics*, *Designs Codes and Cryptography*, *Discrete Mathematics*, *Finite Fields and their Applications*, *Journal of Number Theory*, *International Journal of Computer Mathematics*, *International Journal of Algebra and Computation*

He is also a reviewer for *MathSciNet* and *Zentralblatt MATH*.

6 Expert reviews

Luca Giuzzi has acted as an expert reviewer in the following capacities:

1. 2023: Expert reviewer for the European Research Executive Agency (REA-EU), HORIZON-MSCA-2023-PF-01 AS2.
2. 2023: Expert reviewer for Junior Positions and Associate tenure track positions on behalf of the Le Fonds de la Recherche Scientifique (FNRS), Belgium. per il FNRS (Belgio);
3. 2023: Reviewer for proposals submitted to the project *Galileo2024 – Università Italo-Francese*;
4. 2020: Part of the evaluation board for the admittance to the title of PhD, Università di Modena e Reggio Emilia (IT);
5. 2020: Reviewer of some papers for the VQR 2015-2019 campaign (Italy);
6. 2019: Part of the evaluation board for the award of a tenure track position (Ricercatore RtdB) at Università degli Studi di Brescia (IT);
7. 2018: External referee of a doctoral thesis presented at the University of Melbourne (Australia).

7 Awards and grants

1. May 1997: grant for 'advanced studies abroad' by Università Cattolica
2. July 1997: research grant for 'doctoral studies' by Istituto Nazionale di Alta Matematica; this grant has been renewed for the years 1998-1999 and 1999-2000.
3. September 1997-2000: British EPSRC award (covering tuition fees at Sussex University).
4. June 2000: research grant for 'Progetto e realizzazione di un criptosistema per comunicazioni" (Project and implementation of a cryptosystem for communication systems), POP-FESR 1994/99, Università della Basilicata.
5. September 2000-December 2004: research fellowship at Università degli studi di Brescia.
6. 2001: Exhonerated from compulsory military service as "Citizen involved with special merits in activities of national or international relevance in science, art or culture", Art. 7(d) DLG 504/97.

7. 2015, “Incentivo una tantum anno 2011” (competitive award from the from the University of Brescia for activities in the years 2008-2011).
8. 2017, “Incentivo una tantum anno 2013” (for activities in the years 2011-2013)
9. 2017, FABR (Individual Grant for Basic Research), ANVUR prot. 20/2017, 15 June 2017.

8 Conference organization

1. 2007: Member of the organizing committee of the “XVIII Congresso UMI”, Bari.
2. 2008: Organizer of the international conference “Combinatorics 2008”, Brescia.
3. 2017: Organizer of the international conference “Fq13”, Gaeta.
4. 2017: Organizer of the international conference “HyGraDe”, S. Alessio Siculo (Messina).
5. 2018: Organizer of the international conference “Combinatorics 2018”, Arco (TN).
6. 2020: Organizer of the international conference “Combinatorics 2020”, Mantova (MN).

9 Involvment with National Research Projects (PRIN)

1. 2001: “Strutture geometriche, combinatorica e loro applicazioni”, as member;
2. 2003: “Strutture geometriche, combinatoria e loro applicazioni”, as member;
3. 2005: “Grafi e Geometrie” (2005018845_002), as member;
4. 2008: “Strutture di incidenza e combinatorie” (2008BHF4AW_003), as member;
5. 2012: “Strutture geometriche, combinatoria e loro applicazioni,” (2012XZE22K_009) as Scientific Coordinator of the local research unit.

10 European Projects

1. Participant to COST action IC1104: “Random Network Coding and Designs over GF(q)”

11 Institutional teaching

Prof. Giuzzi has been a *professore aggregato* since September 2006. Since 2018 he is Associate Professor in Geometry.

1. 1998-1999: teaching assistant for Discrete Mathematics at University of Sussex.
2. 1999-2000: teaching assistant for Discrete Mathematics and Group Theory at University of Sussex.
3. 2000-2001: mini-course (10 hours) on cryptography at Università Cattolica del Sacro Cuore.
4. 2001-2002: mini-course on “Cryptography: from DES to AES”, Università di Brescia.
5. 2003-2004: course (10 hours) on ”Discrete Mathematics”, Università di Brescia.
6. 2004-2005: main lecturer for ”Geometria Superiore 2”, Università Cattolica del Sacro Cuore.
7. 2004-2005: teaching assistant at Politecnico di Bari (3 courses).
8. September 2005: introductory course on geometry at Politecnico di Bari (10 hours).
9. 2005-2006: teaching assistant at Politecnico di Bari (3 courses).

10. 2006-2007: main lecturer for "Geometria e Algebra", Mechanical Engineering, A, Politecnico di Bari.
11. 2007-2008: main lecturer for "Geometria e Algebra", Mechanical Engineering, A, Politecnico di Bari.
12. 2007: seminars (3 hours) on Coding Theory at Università degli studi di Brescia, within the European Social Found project n. 411498 Ob. 3 Mis. C3 (2006), 414809, no. 671794 "Corso di alta formazione nell'ambito di dottorati afferenti al settore dell'Ingegneria dell'informazione" (Higher education course for doctoral studies related to information engineering).
13. 2008: co-supervisor for first and second level degree theses in Mathematics at Università Cattolica.
14. 2008-2010: main lecturer for "Complementi di Geometria e Algebra", Università degli Studi di Brescia.
15. 2010-2011: main lecturer for "Algebra per Codici e Crittografia" (Algebra for codes and cryptography), Università degli Studi di Brescia.
16. 2011-2012: main lecturer for
    - "Algebra per Codici e Crittografia", Università degli Studi di Brescia;
    - "Geometria combinatorica" (Combinatorial geometry), Università Cattolica del S. Cuore (BS).
17. 2012-2018: main lecturer for
    - "Algebra per Codici e Crittografia", Università degli Studi di Brescia;
    - "Algebra e Geometria", Università degli studi di Brescia.
18. 2018-2020: professor of
    - "Algebra per Codici e Crittografia" (6 CFU), Università degli Studi di Brescia;
    - "Algebra e Geometria" (9 CFU), Università degli studi di Brescia.
19. 2020-now: professor of
    - "Algebra per Codici e Crittografia" (6 CFU), Università degli Studi di Brescia;
    - "Algebra e Geometria" (9 CFU), Università degli studi di Brescia.
    - "Algebra lineare e geometria analitica"' (6 CFU), Università degli studi di Brescia.

12 Advanced courses

- 2020: advanced Winter School *Mathematics for Engineering Applications*, "Blockchains from bitcoin to robotics — distributed data security for industry 4.0", Politecnico di Bari (IT).
- 2021: Doctoral course "From finite fields to post-quantum cryptography" at Università di Siena (IT).
- 2023: Doctoral course "Data protection: Security, Integrity and Secrecy", Politecnico di Bari (IT).
- 2023: Advanced course "Finite geometry: advanced topics" at *CIMPA-NCM School on Finite Geometry and Coding Theory*, Indian Institute of Technology Hyderabad (IN).

13 Accepted papers

1. I. Cardinali, L. Giuzzi, "Grassmannians of codes", Finite Fields Appl. **94** (2024) 102342 doi:10.1016/j.ffa.2023.102342 (arxiv:2304.08397).
2. A. Aguglia, B. Csajbók, L. Giuzzi, "On regular sets of affine type in finite Desarguesian planes and related codes", Discrete Math. **347** (2024) 113835 doi:10.1016/j.disc.2023.113835 (arxiv:2305.17103)
3. I. Cardinali, L. Giuzzi, "On orthogonal polar spaces", Linear Algebra Appl. 674, 495-518 (2023) doi:10.1016/j.laa.2023.06.013 (arxiv:2301.05876).
4. A. Aguglia, L. Giuzzi, "On the equivalence of certain quasi-Hermitian varieties", J. Combin. Des. 1-15 (2022) doi:10.1002/jcd.21870 (arxiv:2108.04813).

5. I. Cardinali, L. Giuzzi, A. Pasini, "On the generation of some Lie-type geometries", J. Combin. Theory A 193 105673 (2023) doi:10.1016/j.jcta.2022.105673 (arxiv:1912.03484).

6. I. Cardinali, H. Cuypers, L. Giuzzi, A. Pasini, "Characterizations of symplectic polar spaces", Adv. Geom. 23(2) (2023) 281-293 doi:10.1515/advgeom-2023-0006 (arxiv:2205.14426).

7. A. Aguglia, M. Ceria, L. Giuzzi, "Some hypersurfaces over finite fields, minimal codes and secret sharing schemes", Des. Codes. Cryptogr. (2022) doi:10.1007/s10623-022-01051-1 (arxiv:2105.14508).

8. I. Cardinali, L. Giuzzi, A. Pasini, "Nearly all subspaces of a classical polar space arise from its universal embedding", Linear Algebra Appl. 627:287-307 (2021) doi:10.1016/j.laa.2021.06.013 (arxiv:2010.07640).

9. I. Cardinali, L. Giuzzi, M. Kwiatkowski, "On the Grassmann Graph of Linear Codes", Finite Fields Appl. 75:101895 (2021) doi:10.1016/j.ffa.2021.101895 (arxiv:2005.04402).

10. I. Cardinali, L. Giuzzi, A. Pasini, "The generating rank of a polar Grassmannian", Adv. Geom. 21(4):515-539 (2021) (arxiv:1906.10560).

11. A. Aguglia, L. Giuzzi, A. Sonnino, "Near-MDS codes from elliptic curves", Des. Codes Cryptogr. 89: 965-972 (2021) doi:10.1007/s10623-021-00852-0 (arxiv:2009.05623).

12. A. Aguglia, L. Giuzzi, M. Homma, "On Hermitian varieties in PG$(6, q^2)$, Ars Mathematica Contemporanea (2021) doi:10.26493/1855-3974.2358.3c9 (arxiv:2006.04099).

13. I. Cardinali, L. Giuzzi, A. Pasini, "Grassmann embeddings of polar Grassmannians", J. Combin. Theory Series A 170: 105-133 (2020) doi:10.1016/j.jcta.2019.105133 (arxiv:1810.12811).

14. I. Cardinali, L. Giuzzi, "Implementing Line-Hermitian Grassmann codes", Linear Algebra Appl. 580: 96-120 (2019) doi:10.1016/j.laa.2019.06.020 (arxiv:1804.03024).

15. I. Cardinali, L. Giuzzi, "Geometries arising from trilinear forms on low-dimensional vector spaces", Adv. Geom. 19: 269-290 (2019) doi:10.1515/advgeom-2018-0027 (arxiv:1703.06821).

16. L. Giuzzi, F. Zullo, "Identifiers for MRD-codes", Linear Algebra appl. 575: 66-86 (2019) doi:10.1016/j.laa.2019.03.030 (arxiv:1807.09476).

17. I. Cardinali, L. Giuzzi, " Line Hermitian Grassmann Codes and their Parameters", Finite Fields Appl. 51: 407-432 (2018) doi:10.1016/j.ffa.2018.02.006 (arxiv:1706.10255).

18. I. Cardinali, L. Giuzzi, "Minimum distance of Line Orthogonal Grassmann Codes in even characteristic", J. Pure Applied Algebra 222: 2975-2988 (2018) doi:10.1016/j.jpaa.2017.11.009 (arxiv:1605.09333).

19. I. Cardinali, L. Giuzzi, A. Pasini, "On transparent embeddings of point-line geometries", J. Combin. Theory Series A 155: 190-224 (2018) doi:10.1016/j.jcta.2017.11.001 (arxiv:1611.07877).

20. I. Cardinali, L. Giuzzi, "Enumerative Coding for Line Polar Grassmannians with Applications to Codes", Finite Fields Appl. 46: 107-138 (2017) doi:10.1016/j.ffa.2017.03.005 (arxiv:1412.5466).

21. I. Cardinali, L. Giuzzi, A. Pasini, "A geometric approach to alternating k-linear forms", J. Algebraic Combin. 45: 931-963 (2017) doi:10.1007/s10801-016-0730-6 (arxiv:1601.08115).

22. A. Aguglia, L. Giuzzi, "Intersection sets, three-character multisets and associated codes", Des. Codes Cryptogr. 83: 269-282 (2017) doi:10.1007/s10623-016-0302-8 (arxiv:1504.00503).

23. A. Aguglia, L. Giuzzi, "Intersections of the Hermitian Surface with irreducible Quadrics in even Characteristic", Electron. J. Combin. 23 (4): P4.13 (2016) (arxiv:1407.8498).

24. I. Cardinali, L. Giuzzi, K.V. Kaipa, A. Pasini, "Line Polar Grassmann Codes of Orthogonal Type", J. Pure Appl. Algebra 220 (5): 1924-1934 (2016) ISSN: 0022-4049 doi:10.1016/j.jpaa.2015.10.007.

25. I. Cardinali, L. Giuzzi, "Minimum distance of Symplectic Grassmann Codes", Linear Algebra Appl. 488: 124–134 (2016) ISSN: 0024-3795 doi:10.1016/j.laa.2015.09.031 (arxiv:1503.05456).

26. L. Giuzzi, V. Pepe, " On some subvarieties of the Grassmann variety", Linear Multilinear Algebra 63 (11): 2121–2134 (2015) ISSN: 0308-1087 doi:10.1080/03081087.2014.983449 (arxiv:1405.6926).

27. I. Cardinali, L. Giuzzi, "Codes and caps from orthogonal Grassmannians ", Finite Fields Appl. 24: 148–169 (2013) ISSN: 1071-5797 doi:10.1016/j.ffa.2013.07.003 (arxiv:1303.5636).

28. A. Aguglia, L. Giuzzi, "Intersections of the Hermitian surface with irreducible quadrics in $PG(3, q^2)$, q odd", Finite Fields Appl. 30: 1–13 (2014) ISSN: 1071-5797 doi:10.1016/j.ffa.2014.05.005 (arxiv:1307.8386).

29. L. Giuzzi, V. Pepe, "Families of twisted tensor product codes", Des. Codes Cryptogr. 67: 375–384 (2013) ISSN: 0925-1022 doi:10.1007/s10623-012-9613-6 (arxiv:1107.1066).

30. A. Benini, L. Giuzzi, A. Pasotti, "New results on path-decompositions and their down-links", Util. Math. 90: 369–382 (2013) ISSN: 0315-3681 (arxiv:1106.1095).

31. A. Benini, L. Giuzzi, A. Pasotti, "Down-linking (K_v, Γ)–designs to P_3–designs", Util. Math. 90: 3–21 (2013) ISSN: 0315-3681 (arxiv:1004.4127).

32. L. Giuzzi, G. Korchmáros, "Unitals in $PG(2, q^2)$ with a large 2-point stabiliser, Discrete Math. 312 (3): 532–535 (2012), ISSN: 0012-365X doi:10.1016/j.disc.2011.03.017 (arxiv:1009.6109).

33. L. Giuzzi, A. Pasotti, "Sampling complete graphs", Discrete Math. 312 (3), 488–497 (2012), ISSN: 0012-365X, doi:10.1016/j.disc.2011.02.034 (arxiv:0907.3199).

34. A. Aguglia, L. Giuzzi, G. Korchmáros, "Construction of unitals in Desarguesian planes", Discrete Math. 310 (22): 3162–3167 (2010), ISSN: 0012-365X, doi:10.1016/j.disc.2009.06.023 (arxiv:0810.2233).

35. L. Giuzzi, A. Sonnino, "LDPC codes from Singer cycles", Discrete Appl. Math. 157: 1723–1728 (2009), ISSN: 0166-218X, doi:10.1016/j.dam.2009.01.013 (arxiv:0709.2813).

36. A. Aguglia, L. Giuzzi, "On the non–existence of certain hyperovals in dual André planes of order 2^{2k}", Electron. J. Combin. 15(1): N37 (2008); (arxiv:0803.1597).

37. A. Aguglia, L. Giuzzi, G. Korchmáros, "Algebraic curves and maximal arcs", J. Algebraic Combin. 28: 531–544 (2008), ISSN: 0925-9899, doi:10.1007/s10801-008-0122-7 (arxiv:math/0702770).

38. A. Aguglia, L. Giuzzi, "An algorithm for constructing some maximal arcs in PG$(2, q^2)$", Results Math. 52 no. 1–2: 17–33 (2008), ISSN: 1422-6383, doi:10.1007/s00025-007-0268-y (arxiv:math/0611466).

39. A. Aguglia, L. Giuzzi, "Construction of a 3–dimensional MDS code", Contrib. Discrete Math. 3 (1), 39–46 (2007), ISSN: 1715-0868, doi:10.1007/s00025-007-0268-y (arxiv:0708.1558).

40. A. Aguglia, L. Giuzzi, "Orthogonal arrays from Hermitian varieties", Innov. Incidence Geom. 5: 129–144 (2007), ISSN: 1781-6475 (arxiv:0705.3590).

41. L. Giuzzi, "A geometric construction for some ovoids of the Hermitian Surface", Results Math. 49: 81–88 (2006), ISSN: 1422-6383, doi:10.1007/s00025-006-0210-8.

42. L. Giuzzi, "On the intersection of Hermitian surfaces", J. Geom., 85: 49–60 (2006), ISSN: 0047-2468, doi:10.1007/s00022-006-0042-4.

43. L. Giuzzi, G. Korchmáros, "Ovoids of the Hermitian Surface in Odd Characteristic", Adv. Geom., Special Issue (2003), S49–S58, ISSN: 1615-715X.

44. L. Giuzzi, "A characterisation of classical unitals", J. Geom., 74: 86–89 (2002), ISSN: 0047-2468, doi:10.1007/PL00012541.

45. L. Giuzzi, H. Karzel, "Co-Minkowski spaces, their reflection structure and K-loops", Discrete Math. 255: 161–179 (2002), ISSN: 0012-365X, doi:10.1016/S0012-365X(01)00396-X.

46. L. Giuzzi, "Collineation groups of the intersection of two classical unitals", J. Comb. Des. 9: 445–459 (2001) ISSN: 1063-8539, doi:10.1002/jcd.1023.

~

14 Preprints

1. A. Aguglia, L. Giuzzi, V. Siconolfi, "On mutually μ-intersecting quasi-Hermitian varieties with some applications", (arxiv:2406.15589).

2. A. Aguglia, L. Giuzzi, A. Montinaro, V. Siconolfi, "On quasi-Hermitian varieties in even characteristic and related orthogonal arrays", (arxiv:2310.02936)

3. I. Cardinali, L. Giuzzi, A. Pasini, "On the generation of polar grassmannians".

4. L. Giuzzi, A. Sonnino, "Alcune note introduttive sulla crittografia", Quaderno del seminario matematico di Brescia n. 01/2006.
5. L. Giuzzi, "Looking for ovoids of the Hermitian surface: a computational approach", Quaderno del seminario matematico di Brescia n. 33/2002, (arxiv:1210.2600).
6. L. Giuzzi, "Intersections of Hermitian surfaces/2: matrices", Quaderno del seminario matematico di Brescia n. 14/2001.
7. L. Giuzzi, "Intersections of Hermitian surfaces/1: configurations", Quaderno del seminario matematico di Brescia n. 11/2001.
8. L. Giuzzi, "Size of Hermitian intersections", Quaderno del seminario matematico di Brescia n. 07/2001.
9. J.W.P. Hirschfeld, "Algebraic Geometry over a Field of Positive Characteristic - Appunti curati dal dott. L. Giuzzi", Quaderno del seminario matematico di Brescia n. 16/98.

≈

15 Books

1. L. Giuzzi, "Hermitian varieties over finite fields", DPhil thesis under the supervision of Prof. J.W.P. Hirschfeld (University of Sussex).
2. L. Giuzzi, "Codici correttori", UNITEXT Springer Verlag **27** (2006), ISBN: 88–470–0539–6.

≈

16 Proceedings/Extended Abstracts

1. I. Cardinali, L. Giuzzi, "Some results on caps and codes related to orthogonal Grassmannians – a preview", Electron. Notes Discrete Math. 40, 139–144 (2013) ISSN: 1571-0653, doi:10.1016/j.endm.2013.05.026.
2. I. Cardinali, L. Giuzzi, "Polar Grassmannians and their Codes", Extended Abstract accepted for the MEGA2015 conference (2015),(arxiv:1509.07686).

≈

17 Other printed works

1. L. Giuzzi, "Gruppi di Frobenius e strutture geometriche associate" (Frobenius groups and associated geometrical structures, in Italian): *tesi di laurea* at Università Cattolica di Brescia, under the supervision of Prof. S. Pianta.

≈

18 Patents

1. L. Giuzzi, G. Korchmàros, A. Sonnino, "Perfezionamenti nella crittografia a chiave pubblica basata su curve ellittiche", patent no. 0001379714, August 2010.

≈

19 Selected schools and workshops

1. July 1995: "Summer school on combinatorics and finite geometry", Potenza.
2. July 1996 "Summer school Giuseppe Tallini on finite geometry", Brescia.
3. August 1996, "Scuola di Matematica Interuniversitaria", Perugia.
4. September 1997, "Summer school on finite geometry", Potenza.
5. April 1998, Intensive course "Galois Geometry and Generalised Polygons", Ghent.
6. July 1998, "Advanced school on Combinatorial Geometry", Cortona.

7. August 1998, NATO Advanced Study Institute "Difference sets, sequences and their correlation properties", Bad Winsheim.
8. September 1998, "Summer school Giuseppe Tallini on finite geometry", Brescia.
9. November 1998, Workshop "SUNCAGe'98", Caserta.
10. May 1999, summer school "Methods of discrete mathematics: Association schemes, Lattices and Codes", Braunschweig.
11. June 1999, Socrates Intensive programme "Finite geometries and their automorphisms", Potenza.
12. September 1999, "International meeting on coding theory and cryptography", Medina del Campo (ES).
13. October 2000, "ECC 2000: 4th workshop on elliptic curve cryptography", Essen.
14. May 2001, "CHES 2001: Workshop on cryptographic hardware and embedded solutions", Paris.
15. July 2002, "Summer school Giuseppe Tallini" on finite geometry, Brescia.
16. September 2005, "Summer school Giuseppe Tallini on Combinatorial Geometries", Potenza.
17. 10–16 September 2006, "Second Irsee Conference on Finite Geometries", Irsee (DE).
18. 24–29 September 2007, "XVIII Congresso UMI", Bari (IT).
19. 22–28 June 2008, "Combinatorics 2008", Brescia (IT).
20. 13–17 June 2009, "Fq9 – Finite Fields and their Applications", Shannon Institute, Dublin (IE).
21. 30 May – 4 June 2010, "Fourth Pythagorean Conference", Corfu (GR).
22. 5–11 June 2010, NATO Advanced Study Institute, "Information Security and Related Combinatorics", Opatija (HR).
23. 27 June – 3 July 2010, "Combinatorics 2010", Verbania (IT).
24. 19–25 June 2011, "Third Irsee Conference on Finite Geometries", Irsee (DE).
25. 10–16 July 2011, "Fq10 – Finite Fields and their Applications", Ghent (BE).
26. 6–10 February 2012, "Incidenge geometry and buildings", Ghent (BE).
27. 13–14 February 2012, "Giornate di Geometria", Vicenza (IT).
28. 9–15 September 2012, "Combinatorics 2012", Perugia (IT).

20 Conference talks

1. 6 November 1997, "Spazi co–Minkowski e loro struttura di riflessione", GNSAGA national meeting, Perugia (IT).
2. 19 June 1998, "Co-Minkowski spaces and their reflection structure", Combinatorics '98, Palermo (IT).
3. 31 May 2000, "Intersection numbers for Hermitian varieties", Combinatorics 2000, Gaeta (IT).
4. 19 July 2000, "Groups stabilising the intersection of two classical unitals", Fourth Isle of Thorns conference of finite geometries (invited participation), Isle of Thorns (UK).
5. 5 July 2001, "A short characterisation of classical unitals", 18th British Combinatorial Conference, Brighton.
6. 8 June 2002, "Ovoids of the Hermitian surface", Combinatorics 2002, Maratea (IT).
7. 3 October 2003, "A family of ovoids of the Hermitian Surface in $PG(3, q^2)$ with odd $q \geq 5$", International Symposium on Graphs, Designs and Applications 2003, Messina (IT).
8. 26 June 2006, "LDPC Codes from Projective Spaces", Combinatorics 2006, Ischia (IT).
9. 30 January 2010, invited speaker, "Geometry and codes", workshop in honour of Prof. M. Marchi, on occasion of his 70th birthday.

10. 29 June 2010, "On samplings of graphs", Combinatorics 2010, Verbania (IT).
11. 12 July 2011, "Unitals in $PG(2, q^2)$ with a large 2-point stabiliser", Fq10 — 10th International Conference of Finite Fields and their Applications, Ghent (BE).
12. 10 September 2012, "Caps and codes from Polar Grassmannians", Combinatorics 2012, Perugia (IT).
13. 19 September 2013, "Linear codes from orthogonal Grassmannians", Conference on Random network codes and Designs, Ghent (BE).
14. 5 June 2014, "On Line Polar Grassmann Codes", Combinatorics 2014, Gaeta (IT).
15. 19 June 2014, "Linear Polar Grassmann Codes", Algebra, codes and Networks, Bordeaux (FR).
16. 18 September 2014, "Intersection of Hermitian Surfaces and quadrics", Finite Geometries — Fourth IRSEE conference (invited participation), Kloster Irsee (DE).
17. 16 March 2015, "Polar Grassmann codes — Part II", ALCOMA15, Kloster Banz (DE).
18. 19 June 2015, "Polar Grassmannians and their Codes", MEGA2015, Trento (IT).
19. 3 June 2016, "Implementing Polar Graßmann Codes", Combinatorics 2016, Maratea (IT).
20. June 2017, "Hermitian Line Polar Graßmann Codes", Fq13, Gaeta (IT).
21. September 2017, "Transparent embeddings of point-line geometries", Fifth Irsee Conference (invited participation), Kloster Irsee (DE).
22. September 2019, "Generating and embedding polar Grassmannians", Buildings 2019, Magdeburg (DE).
23. August 2022, "On subspaces of classical polar spaces", Finite Geometries 2022 — Sixth Irsee Conference (invited participation), Irsee (DE).
24. September 2022, "On symplectic polar spaces", Polygons, buildings and related geometries, Ghent (BE).
25. January 2023, invited speaker, "Grassmannians, their embeddings and applications", GL70 — A conference in honor of Guglielmo Lunardon, Naples (IT).
26. February 2023, "Linear codes and Grassmann graphs", Conference on Algebraic varieties over finite fields and Algebraic geometry codes (COGNAC) (invited participation), Marseille (FR).
27. December 2023, invited speaker, "On orthogonal polar spaces", International Conference on Algebraic Geometry, Coding Theory and Combinatorics, Indian Institute of Technology Hyderabad (IN).

21 Seminars

All the seminars in this section have been given upon invitation by the hosting institutions.

1. June 1997, "Kinematic spaces derived from Frobenius Groups", School of Mathematical Sciences, University of Sussex.
2. 23 and 24 September 1998, "Cryptography and finite geometries (I and II)", Mathematics department at Università Cattolica del Sacro Cuore, Brescia.
3. 16 October 1998, "Public-key cryptosystems and elliptic curves", School of Mathematical Sciences, University of Sussex, Brighton.
4. 24 November 1999, "Of entropy and keys", School of Mathematical Sciences, University of Sussex, Brighton.
5. 10 February 2000, public seminar in "Trust, information and privacy: theory of *secret writings* and their legal issues", Università Cattolica del Sacro Cuore, Brescia.
6. 23 May 2001, "Intersection of Hermitian varieties", Università di Brescia.
7. 5 December 2001, "Hermitian varieties over finite fields: why?", Università Cattolica del Sacro Cuore, Brescia.
8. 10 April 2002, "Caps and ovoids in the Hermitian surface: a comutational approach", Università di Brescia.

9. 11 July 2002, "An introduction to modern cryptography: from RSA to AES", Summer School "Giuseppe Tallini" 2002, Brescia.

10. 5 February 2003, "Introduction to Coding theory", Università Cattolica del Sacro Cuore, Brescia.

11. 12 February 2003, "From Codes to Designs", Università Cattolica del Sacro Cuore, Brescia.

12. 6 November 2003, "Incidence configurations in the Hermitian surface", Giornate di Geometria, Università Cattolica del Sacro Cuore, Brescia.

13. 20 November 2003, "Mathematics plus secrecy", Museum of Sciences, Brescia.

14. 4 May 2004, "Finite geometry and Cryptography", Politecnico di Bari.

15. 6 May 2004, "Finite fields in C++", Dipartimento di Matematica, Università di Napoli.

16. 9 September 2005, "A defense of cryptography", Università della Basilicata.

17. 29 May 2006 and 31 May 2006, "An introduction to algebraic decoding of cyclic codes", Facoltà di Ingegneria, Università di Brescia.

18. 25 October 2006, "Security, privacy and secrecy: several faces of cryptography", Dipartimento di matematica, Università di Bari.

19. 21 November 2006, "Reed–Solomon codes", Facoltà di Ingegneria, Università di Brescia.

20. 23 Novembre 2006, "Cryptography of (in)security", Facoltà di Ingegneria, Università di Brescia.

21. 4 and 6 December 2006, "Uses of cryptography: from secrecy to security", Facoltà di Economia di Bari.

22. 5 December 2008, "Elliptic Curves: theory", Università Cattolica, Brescia

23. 13 February 2009, "Elliptic Curves: practice", Università Cattolica, Brescia.

24. 8 April 2009, "Non–binary BCH codes", Dipartimento di Matematica, Università Federico II, Napoli.

25. 30 January 2010, "Geometry and codes", Worshop in honor of M.Marchi, Università Cattolica, Brescia.

26. 29 October 2010, "Mathematics and secrets", Università Cattolica, Brescia.

27. From 15 till 21 May 2011 L. Giuzzi has been a guest of the Mathematics Department of the University of Gent (BE).

28. 15 March 2012, "Non–linear codes", Dipartimento di Matematica, Università Federico II, Napoli.

29. 24 April 2012, "Algebraic and geometric methods in cryptography", Dipartimento di Matematica, Politecnico di Milano.

30. 21 January 2014, "Strutture geometriche, combinatorica ed applicazioni", DICATAM, Università di Brescia.

31. 28 May 2019, "Polar Grassmannians", Università di Siena.

22 Summary of research interests

1. Incidence geometries.

2. Coding theory and Cryptography.

3. Finite geometries and varieties over finite fields.

23 Computer skills

1. Very good knowledge of Linux (since 1994);
2. Experience as system administrator of Solaris (from 2.5 up to 2.8) and Digital Unix (4.0A - 4.0E) systems;
3. Good knowledge of C and C++; knowledge of Julia.
4. Good knowledge of HTML, XHTML and CSS;
5. Working knowledge of several Computer Algebra systems.

24 Abstracts of the main papers

▷ Hermitian varieties over finite fields
L. Giuzzi, University of Sussex (2000)

A projective space $\mathrm{PG}(n,q)$ admits at most three types of polarity: orthogonal, symplectic and unitary. The absolute points of an orthogonal polarity constitute a non-degenerate quadric in $\mathrm{PG}(n,q)$; for a symplectic polarity, all the points of $\mathrm{PG}(n,2^t)$ are absolute; the locus of all absolute points of a unitary polarity is a non-degenerate Hermitian variety.

Non-degenerate Hermitian varieties are unique in $\mathrm{PG}(n,q)$ up to projectivities. However, two distinct Hermitian varieties might intersect in many different configurations. Our aim in this thesis is to study such configurations in some detail.

In Chapter 1 we introduce some background material on finite fields, projective spaces, collineation groups and Hermitian varieties.

Chapter 2 deals with the two-dimensional case. Kestenband has proven that two Hermitian curves may meet in any of seven point-line configurations. In Section 2.1, we present this classification. In Section 2.2, we verify that any two configurations belonging to the same class are, in fact, projectively equivalent and we determine the linear collineation group stabilizing each of them. Such a group is usually quite large and is transitive on almost all the points of the intersection. A subset U of $\mathrm{PG}(2,q)$ such that any line of the plane meets U in either 1 or $\sqrt{q}+1$ points is called a *unital*. A Hermitian curve is a *classical unital*. However, there exist non-classical unitals as well. In Section 2.3 we present a short proof of a characterisation of the Hermitian curve as the unital stabilized by a Singer subgroup of order $q-\sqrt{q}+1$.

In Chapter 3, we describe the point-line-plane configurations arising in dimension 3 from intersecting two Hermitian surfaces. Our approach consists first in determining some combinatorial properties the configurations have to satisfy and then in actually constructing all the possible cases. Section 3.1 presents the list of all possible intersection classes; after some more technical results in Section 3.2, in Section 3.3 we construct linear systems of Hermitian surfaces yielding the wanted configurations for any class. In this chapter we deal with intersections which contain at least $\sqrt{q}+1$ points on a line.

Chapter 4 is divided into two independent sections: in Section 4.1 we study the determinantal variety of all the $(n+1)\times(n+1)$ Hermitian matrices as a hypersurface of $\mathrm{PG}(n^2+2n,\sqrt{q})$. From the study of such a variety we are able to determine the list of all possible intersection sizes for any dimension n. In Section 4.2 we present some computer code in order to produce pencils of Hermitian varieties in $\mathrm{PG}(n,q)$. This code, however, is able to provide useful results only for small values of n and q. Some possible improvements, both from the theoretic standpoint and the computational one, are suggested.

▷ Codici Correttori
L. Giuzzi, UNITEXT Springer Verlag **27** (2006)

This book (in italian) is a self-contained introduction to coding theory for undergraduate students in engineering, mathematics or computer science. The main topics are

1. The theory of linear block codes, with special regards to algebraic constructions and algebraic decoding;
2. Construction of codes from designs and links between projective geometry and coding theory;
3. Asymptotic bounds;
4. An introduction to Algebraic-Geometry codes;
5. LDPC codes and Tanner graphs;
6. Convolutory codes.

▷ Collineation Groups of the Intersection of Two Classical Unitals
L. Giuzzi, J. Comb. Des. 9: 445–459 (2001).

Kestenband proved that there are only seven pairwise non-isomorphic Hermitian intersections in the Desarguesian projective plane $\mathrm{PG}(2, q^2)$ of square order q^2. His classification is based on the study of the minimal polynomials of the matrices associated with the curves and leads to results of purely combinatorial nature: in fact, two Hermitian intersections from the same class might not be projectively equivalent in $\mathrm{PG}(2, q^2)$ and might have different collineation groups. The projective classification of Hermitian intersections in $\mathrm{PG}(2, q^2)$ is the main goal in this paper. It turns out that each of Kestenband's classes consists of projectively equivalent Hermitian intersections. A complete classification of the linear collineation groups preserving a Hermitian intersection is also given.

▷ Co-Minkowski Spaces, their Reflection Structure and K-loops
L.Giuzzi, H. Karzel, Discrete Math. 255: 161–179 (2002).

In this work an infinite family of K-loops is constructed from the reflection structure of co-Minkowski planes and their properties are analysed.

▷ A Characterisation of Classical Unitals
L. Giuzzi, J. Geom., 74: 86–89 (2002).

A short proof is given of the following result: *A unital in* $\mathrm{PG}(2, q)$ *is classical if and only if it is preserved by a cyclic linear collineation group of order* $q - \sqrt{q} + 1$.

▷ Ovoids of the Hermitian Surface in Odd Characteristic
L. Giuzzi, G. Korchmáros, Adv. Geom., Special Issue (2003), S49–S58.

We construct a new ovoid of the polar space arising from the Hermitian surface of $\mathrm{PG}(3, q^2)$ with $q \geq 5$ odd. The automorphism group Γ of such an ovoid has a normal cyclic subgroup Φ of order $\frac{1}{2}(q+1)$ such that $\Gamma/\Phi \cong \mathrm{PGL}(2, q)$. Furthermore, Γ has three orbits on the ovoid, one of size $q+1$ and two of size $\frac{1}{2}q(q-1)(q+1)$.

▷ On the Intersection of Hermitian Surfaces
L. Giuzzi, J. Geom., 85: 49–60 (2006).

We provide a description of the configuration arising from intersection of two Hermitian surfaces in $\mathrm{PG}(3, q)$, provided that the linear system they generate contains at least a degenerate variety.

▷ A Geometric Construction for Some Ovoids of the Hermitian Surface
L. Giuzzi, Results Math. 49: 81–88 (2006).

Multiple derivation of the classical ovoid of the Hermitian surface $\mathscr{H}(3, q^2)$ of $\mathrm{PG}(3, q^2)$ is a well known, powerful method for constructing large families of non classical ovoids of $\mathscr{H}(3, q^2)$. In this paper, multiple derivation is generalised and applied to non-classical ovoids. A resulting new family of ovoids is investigated.

▷ Orthogonal Arrays from Hermitian Varieties
A. Aguglia, L. Giuzzi, Innov. Incidence Geom. 5: 129–144 (2007).

A simple orthogonal array $\mathrm{OA}(q^{2n-1}, q^{2n-2}, q, 2)$ is constructed by using the action of a large subgroup of $\mathrm{PGL}(n+1, q^2)$ on a set of non–degenerate Hermitian varieties in $\mathrm{PG}(n, q^2)$.

▷ Construction of a 3–dimensional MDS Code
A. Aguglia, L. Giuzzi, Contrib. Discrete Math. 3 (1), 39–46 (2007).

In this paper, we describe a procedure for constructing q-ary $[N, 3, N-2]$-MDS codes, of length $N \leq q+1$ (for q odd) or $N \leq q+2$ (for q even), using a set of non-degenerate Hermitian forms in $\mathrm{PG}(2, q^2)$.

▷ An Algorithm for Constructing some Maximal Arcs in $\mathrm{PG}(2, q^2)$
A. Aguglia, L. Giuzzi, Results Math. 52 no. 1–2: 17–33 (2008).

In 1974, J. Thas constructed a new class of maximal arcs for the Desarguesian plane of order q^2. The construction relied upon the existence of a regular spread of tangent lines to an ovoid in $\mathrm{PG}(3, q)$ and, in particular, it does apply to the Suzuki-Tits ovoid. In this paper, we describe an algorithm for obtaining a possible representation of such arcs in $\mathrm{PG}(2, q^2)$.

▷ Algebraic Curves and Maximal Arcs

A. Aguglia, L. Giuzzi, G. Korchmáros, J. Algebraic Combin. 28: 531–544 (2008)/

A lower bound on the minimum degree of the plane algebraic curves containing every point in a large point-set $\mathscr{K}$ of the Desarguesian plane $\mathrm{PG}(2,q)$ is obtained. The case where $\mathscr{K}$ is a maximal (k,n)-arc is considered to greater extent.

▷ On the Non-existence of Certain Hyperovals in Dual André Planes of Order 2^{2k}

A. Aguglia, L. Giuzzi, Electron. J. Combin. 15(1): N37 (2008).

No oval contained in a regular hyperoval of the Desarguesian plane $\mathrm{PG}(2,q^2)$, q even, is inherited by a Moulton plane of order q^2.

▷ LDPC Codes from Singer Cycles

L. Giuzzi, A. Sonnino, Discrete Appl. Math. 157: 1723–1728 (2009).

The main goal of coding theory is to devise efficient systems to exploit the full capacity of a communication channel, thus achieving an arbitrarily small error probability. Low Density Parity Check (LDPC) codes are a family of block codes – characterised by admitting a sparse parity check matrix – with good correction capabilities. In the present paper the orbits of subspaces of a finite projective space under the action of a Singer cycle are investigated. The incidence matrix associated to each of these structures yields an LDPC code in a natural manner.

▷ Construction of Unitals in Desarguesian Planes

A. Aguglia, L. Giuzzi, G. Korchmáros, Discrete Math. 310 (22): 3162–3167 (2010).

We present a new construction of non-classical unitals from a classical unital $\mathscr{U}$ in $\mathrm{PG}(2,q^2)$. The resulting non-classical unitals are B–M unitals. The idea is to find a non-standard model Π of $\mathrm{PG}(2,q^2)$ with the following three properties:

1. points of Π are those of $\mathrm{PG}(2,q^2)$;
2. lines of Π are certain lines and conics of $\mathrm{PG}(2,q^2)$;
3. the points in $\mathscr{U}$ form a non-classical B-M unital in Π.

Our construction also works for the B-T unital, provided that conics are replaced by certain algebraic curves of higher degree.

▷ Sampling Complete Graphs

L. Giuzzi, A. Pasotti, Discrete Math. 312 (3), 488–497 (2012).

In the present paper, complete designs of graphs are considered. The notion of (regular) sampling is introduced and analyzed in detail, showing that the trivial necessary condition for its existence is actually sufficient. Some examples are also provided.

▷ Unitals in $\mathrm{PG}(2,q^2)$ with a large 2–point Stabiliser

L. Giuzzi, G. Korchmáros, Discrete Math. 312 (3): 532–535 (2012).

Let $\mathscr{U}$ be a unital embedded in the Desarguesian projective plane $\mathrm{PG}(2,q^2)$. Write M for the subgroup of $\mathrm{PGL}(3,q^2)$ which preserves $\mathscr{U}$. We show that $\mathscr{U}$ is classical if and only if $\mathscr{U}$ has two distinct points P,Q for which the stabiliser $G=M_{P,Q}$ has order q^2-1.

▷ Down–linking (K_v,Γ)-designs to P_3-designs

A. Benini, L. Giuzzi, A. Pasotti, Util. Math. 90: 3–21 (2013).

Let Γ' be a subgraph of a graph Γ. We define a down-link from a (K_v,Γ)-design $\mathscr{B}$ to a (K_n,Γ')-design $\mathscr{B}'$ as a map $f:\mathscr{B}$
$to\mathscr{B}'$ mapping any block of $\mathscr{B}$ into one of its subgraphs. This is a new concept, closely related with both the notion of metamorphosis and that of embedding. In the present paper we study down-links in general and prove that any (K_v,Γ)-design might be down-linked to a (K_n,Γ')-design, provided that n is admissible and large enough. We also show that if $\Gamma'=P_3$, it is always possible to find a down-link to a design of order at most $v+3$. This bound is then improved for several classes of graphs Γ, by providing explicit constructions.

▷ New Results on Path–decompositions and their Down-links

A. Benini, L. Giuzzi, A. Pasotti, Util. Math. 90: 369-382 (2013).

"In "A. Benini, L. Giuzzi, A. Pasotti, *Down–linking (K_v,Γ)-designs to P_3-designs*, Util. Math. 90: 3–21 (2013)", the concept of down-link from a (K_v,Γ)-design $\mathscr{B}$ to a (K_n,Γ')-design $\mathscr{B}'$ has been introduced. In the present paper the

spectrum problems for $\Gamma' = P_4$ are studied. General results on the existence of path-decompositions and embeddings between path-decompositions playing a fundamental role for the construction of down-links are also presented.

▷ Families of Twisted Tensor Product Codes
L. Giuzzi, V. Pepe, Des. Codes Cryptogr. 67: 375–384 (2013).

Using geometric properties of the variety $\mathscr{V}_{r,t}$, the image under the Grassmannian map of a Desarguesian $(t-1)$-spread of $\mathrm{PG}(rt-1,q)$, we introduce error correcting codes related to the twisted tensor product construction, producing several families of constacyclic codes. We determine the precise parameters of these codes and characterise the words of minimum weight.

▷ Caps and Codes from Orthogonal Grassmannians
I. Cardinali, L. Giuzzi, Finite Fields Appl. 24: 148–169 (2013).

In this paper we investigate linear error correcting codes and projective caps related to the Grassmann embedding ε_k^{gr} of an orthogonal Grassmannian Δ_k. In particular, we determine some of the parameters of the codes arising from the projective system determined by $\varepsilon_k^{gr}(\Delta_k)$. We also study special sets of points of Δ_k which are met by any line of Δ_k in at most 2 points and we show that their image under the Grassmann embedding ε_k^{gr} is a projective cap.

▷ Intersections of the Hermitian Surface with Irreducible Quadrics in $\mathrm{PG}(3,q^2)$, q Odd
A. Aguglia, L. Giuzzi, Finite Fields Appl. 30: 1–13 (2014).

In $\mathrm{PG}(3,q^2)$, with q odd, we determine the possible intersection sizes of a Hermitian surface $\mathscr{H}$ and an irreducible quadric $\mathscr{Q}$ having the same tangent plane π at a common point $P \in \mathscr{Q} \cap \mathscr{H}$.

▷ On some Subvarieties of the Grassmann Variety
L. Giuzzi, V. Pepe, Linear Multilinear Algebra 63 (11): 2121–2134 (2015).

Let $\mathscr{S}$ be a Desarguesian $(t-1)$-spread of $\mathrm{PG}(rt-1,q)$, Π a m–dimensional subspace of $\mathrm{PG}(rt-1,q)$ and Λ the linear set consisting of the elements of $\mathscr{S}$ with non-empty intersection with Π. It is known that the Plücker embedding of the elements of $\mathscr{S}$ is a variety of $\mathrm{PG}(r^t-1,q)$, say $\mathscr{V}_{rt}$. In this paper, we describe the image under the Plücker embedding of the elements of Λ and we show that it is an m-dimensional algebraic variety, projection of a Veronese variety of dimension m and degree t, and it is a suitable linear section of $\mathscr{V}_{rt}$.

▷ Minimum Distance of Symplectic Grassmann Codes
I. Cardinali, L. Giuzzi, Linear Algebra Appl. 488: 124–134 (2016).

In this paper we introduce symplectic Grassmann codes, in analogy to ordinary Grassmann codes and orthogonal Grassmann codes, as projective codes defined by symplectic Grassmannians. Lagrangian-Grassmannian codes are a special class of symplectic Grassmann codes. We describe all the parameters of line symplectic Grassmann codes and we provide the full weight enumerator for the Lagrangian-Grassmannian codes of rank 2 and 3.

▷ Line Polar Grassmann Codes of Orthogonal Type
I. Cardinali, L. Giuzzi, K.V. Kaipa, A. Pasini, J. Pure Appl. Algebra 220 (5): 1924-1934 (2016).

Polar Grassmann codes of orthogonal type have been introduced in "I. Cardinali, L. Giuzzi, *Codes and Caps from Orthogonal Grassmannians*, Finite Fields Appl. 24: 148-169 (2013), doi:10.1016/j.ffa.2013.07.003". They are subcodes of the Grassmann code arising from the projective system defined by the Plücker embedding of a polar Grassmannian of orthogonal type. In the present paper we fully determine the minimum distance of line polar Grassmann Codes of orthogonal type for q odd.

▷ Intersections of the Hermitian Surface with Irreducible Quadrics in Even Characteristic
A. Aguglia, L. Giuzzi, Electron. J. Combin. 23 (4): P4.13 (2016).

We determine the possible intersection sizes of a Hermitian surface $\mathscr{H}$ with an irreducible quadric of $\mathrm{PG}(3,q^2)$ sharing at least a tangent plane at a common non-singular point when q is even.

▷ Intersection Sets, Three-character Multisets and Associated Codes
A. Aguglia, L. Giuzzi, Des. Codes Cryptogr. 83: 269-282 (2017).

In this article we construct new minimal intersection sets in $\mathrm{AG}(r,q^2)$ sporting three intersection numbers with hyperplanes; we then use these sets to obtain linear error correcting codes with few weights, whose weight enumerator we also determine. Furthermore, we provide a new family of three-character multisets in $\mathrm{PG}(r,q^2)$ with r even and we also compute their weight distribution.

▷ A Geometric Approach to Alternating k-linear Forms

I. Cardinali, L. Giuzzi, A. Pasini, J. Algebraic Combin. 45: 931-963 (2017).

Given an n-dimensional vector space V over a field $\mathbb{K}$, let $2 \leq k < n$. A natural one-to-one correspondence exists between the alternating k-linear forms of V and the linear functionals of $\bigwedge^k V$, an alternating k-linear form φ and a linear functional f being matched in this correspondence precisely when $\varphi(x_1, \ldots, x_k) = f(x_1 \wedge \cdots \wedge x_k)$ for all $x_1, \ldots, x_k \in V$. Let $\varepsilon_k : \mathscr{G}_k(V) \to \mathrm{PG}(\bigwedge^k V)$ be the Plücker embedding of the k-Grassmannian $\mathscr{G}_k(V)$ of V. Then $\varepsilon_k^{-1}(\ker(f) \cap \varepsilon_k(\mathscr{G}_k(V)))$ is a hyperplane of the point-line geometry $\mathscr{G}_k(V)$. It is well known that all hyperplanes of $\mathscr{G}_k(V)$ can be obtained in this way, namely every hyperplane of $\mathscr{G}_k(V)$ is the family of k-subspaces of V where a given alternating k-linear form identically vanishes. For a hyperplane H of $\mathscr{G}_k(V)$, let $R^\uparrow(H)$ be the subset (in fact a subspace) of $\mathscr{G}_{k-1}(V)$ formed by the $(k-1)$-subspaces $A \subset V$ such that H contains all k-subspaces that contain A. In other words, if φ is the (unique modulo a scalar) alternating k-linear form defining H, then the elements of $R^\uparrow(H)$ are the $(k-1)$-subspaces $A = \langle a_1, \ldots, a_{k-1} \rangle$ of V such that $\varphi(a_1, \ldots, a_{k-1}, x) = 0$ for all $x \in V$. In principle, when $n-k$ is even it might happen that $R^\uparrow(H) = \emptyset$. When $n-k$ is odd then $R^\uparrow(H) \neq \emptyset$, since every $(k-2)$-subspace of V is contained in at least one member of $R^\uparrow(H)$, but it can happen that every $(k-2)$-subspace of V is contained in precisely one member of $R^\uparrow(H)$. If this is the case, we say that $R^\uparrow(H)$ is *spread-like*. In this paper we obtain some results on $R^\uparrow(H)$ which answer some open questions from the literature and suggest the conjecture that, if $n-k$ is even and at least 4, then $R^\uparrow(H) \neq \emptyset$ but for one exception with $\mathbb{K} \leq \mathbb{R}$ and $(n,k) = (7,3)$, while if $n-k$ is odd and at least 5 then $R^\uparrow(H)$ is never spread-like.

▷ Minimum distance of Line Orthogonal Grassmann Codes in even characteristic

I. Cardinali, L. Giuzzi, J. Pure Applied Algebra 222 (10): 2975-2988 (2018)

In this paper we determine the minimum distance of orthogonal line-Grassmann codes for q even. The case q odd was solved in "I. Cardinali, L. Giuzzi, K. Kaipa, A. Pasini, Line Polar Grassmann Codes of Orthogonal Type, J. Pure Applied Algebra doi:10.1016/j.jpaa.2015.10.007) We also show that for q even all minimum weight codewords are equivalent and that symplectic line-Grassmann codes are proper subcodes of codimension $2n$ of the orthogonal ones.

▷ Enumerative coding for Line Polar Grassmannians with applications to codes

I. Cardinali, L. Giuzzi, Finite Fields Appl. 46: 107-138 (2017)

A k-polar Grassmannian is the geometry having as pointset the set of all k-dimensional subspaces of a vector space V which are totally isotropic for a given non-degenerate bilinear form μ defined on V. Hence it can be regarded as a subgeometry of the ordinary k-Grassmannian. In this paper we deal with orthogonal line Grassmannians and with symplectic line Grassmannians, i.e. we assume $k = 2$ and μ a non-degenerate symmetric or alternating form. We will provide a method to efficiently enumerate the pointsets of both orthogonal and symplectic line Grassmannians. This has several nice applications; among them, we shall discuss an efficient encoding/decoding/error correction strategy for line polar Grassmann codes of both types.

▷ On transparent embeddings of point-line geometries

I. Cardinali, L. Giuzzi, A. Pasini, J. Combin Theory Series A 155: 190-224 (2018)

We introduce the class of transparent embeddings for a point-line geometry $\Gamma = (\mathscr{P}, \mathscr{L})$ as the class of full projective embeddings ε of Γ such that the preimage of any projective line fully contained in $\varepsilon(\mathscr{P})$ is a line of Γ. We will then investigate the transparency of Plücker embeddings of projective and polar grassmannians and spin embeddings of half-spin geometries and dual polar spaces of orthogonal type. As an application of our results on transparency, we will derive several Chow-like theorems for polar grassmannians and half-spin geometries.

▷ Line Hermitian Grassmann Codes and their Parameters

I. Cardinali, L. Giuzzi, Finite Fields Appl. 51: 407-432 (2018)

In this paper we introduce and study line Hermitian Grassmann codes as those subcodes of the Grassmann codes associated to the 2-Grassmannian of a Hermitian polar space defined over a finite field of square order. In particular, we determine their parameters and characterize the words of minimum weight.

▷ Identifiers for MRD codes

L. Giuzzi, F. Zullo, Linear Algebra Appl. 575: 66-86 (2019)

For any admissible value of the parameters n and k there exist $[n,k]$-Maximum Rank distance $\mathbb{F}_q$-linear codes. Indeed, it can be shown that if field extensions large enough are considered, almost all rank distance codes are MRD. On the other hand, very few families up to equivalence of such codes are currently known. In the present paper we study some invariants of MRD codes and evaluate their value for the known families, providing a new characterization of generalized twisted Gabidulin codes.

▷ Geometries arising from trilinear forms on low-dimensional vector spaces

I. Cardinali, L. Giuzzi, Adv. Geom 19(2): 269-290 (2019)

Let $\mathscr{G}_k(V)$ be the k-Grassmannian of a vector space V with $\dim V = n$. Given a hyperplane H of $\mathscr{G}_k(V)$, we define in [I. Cardinali, L. Giuzzi, A. Pasini, A geometric approach to alternating k-linear forms, J. Algebraic Combin. doi:10.1007/s10801-016-0730-6] a point-line subgeometry of $\mathrm{PG}(V)$ called the *geometry of poles of* H. In the present paper, exploiting the classification of alternating trilinear forms in low dimension, we characterize the possible geometries of poles arising for $k = 3$ and $n \leq 7$ and propose some new constructions. We also extend a result of [J.Draisma, R. Shaw, Singular lines of trilinear forms, Linear Algebra Appl. doi:10.1016/j.laa.2010.03.040] regarding the existence of line spreads of $\mathrm{PG}(5, \mathbb{K})$ arising from hyperplanes of $\mathscr{G}_3(V)$.

▷ Implementing Line-Hermitian Grassmann codes

I. Cardinali, L. Giuzzi, Linear Algebra Appl. 580: 96-120 (2019) doi:10.1016/j.laa.2019.06.020 (arxiv:1804.03024)

In [I. Cardinali and L. Giuzzi. Line Hermitian Grassmann codes and their parameters. Finite Fields Appl., 51: 407-432, 2018] we introduced line Hermitian Grassmann codes and determined their parameters. The aim of this paper is to present (in the spirit of [I. Cardinali and L. Giuzzi. Enumerative coding for line polar Grassmannians with applications to codes. Finite Fields Appl., 46:107-138, 2017]) an algorithm for the point enumerator of a line Hermitian Grassmannian which can be usefully applied to get efficient encoders, decoders and error correction algorithms for the aforementioned codes.

▷ Grassmann embeddings of polar Grassmannians

I. Cardinali, L. Giuzzi, A. Pasini, J. Combin. Theory Series A 170: 105-133 (2020) doi:10.1016/j.jcta.2019.105133 (arxiv:1810.12811)

In this paper we compute the dimension of the Grassmann embeddings of the polar Grassmannians associated to a possibly degenerate Hermitian, alternating or quadratic form with possibly non-maximal Witt index. Moreover, in the characteristic 2 case, when the form is quadratic and non-degenerate with bilinearization of minimal Witt index, we define a generalization of the so-called Weyl embedding (see [I. Cardinali and A. Pasini, Grassmann and Weyl embeddings of orthogonal Grassmannians. J. Algebr. Combin. 38 (2013), 863-888]) and prove that the Grassmann embedding is a quotient of this generalized 'Weyl-like' embedding. We also estimate the dimension of the latter.

▷ Near-MDS codes from elliptic curves

A. Aguglia, L. Giuzzi, A. Sonnino, Des. Codes. Cryptogr. 89: 965-972 (2021) doi:10.1007/s10623-021-00852-0 (arxiv:2009.05623)

We provide a new construction of $[n, 9, n-9]_q$ near-MDS codes arising from elliptic curves with n $\mathbb{F}_q$-rational points. Furthermore we show that in some cases these codes cannot be extended to longer near-MDS codes.

▷ On Hermitian varieties in $\mathrm{PG}(6, q^2)$

A. Aguglia, L. Giuzzi, M. Homma, Ars Mathematica Contemporanea (2021) doi:10.26493/1855-3974.2358.3c9 (arxiv:2006.04099)

In this paper we characterize the non-singular Hermitian variety $\mathscr{H}(6, q^2)$ of $\mathrm{PG}(6, q^2)$, $q \neq 2$ among the irreducible hypersurfaces of degree $q + 1$ in $\mathrm{PG}(6, q^2)$ not containing solids by the number of its points and the existence of a solid S meeting it in $q^4 + q^2 + 1$ points.

▷ The generating rank of a polar Grassmannian

I. Cardinali, L. Giuzzi, A. Pasini, Adv. Geom. 21:4 (2021) 515-539 doi:10.1515/advgeom-2021-0022 (arxiv:1906.10560)

In this paper we compute the generating rank of k-polar Grassmannians defined over commutative division rings. Among the new results, we compute the generating rank of k-Grassmannians arising from Hermitian forms of Witt index n defined over vector spaces of dimension $N > 2n$. We also study generating sets for the 2-Grassmannians arising from quadratic forms of Witt index n defined over $V(N, \mathbb{F}_q)$ for $q = 4, 8, 9$ and $2n \leq N \leq 2n + 2$. We prove that for N>6 they can be generated over the prime subfield, thus determining their generating rank.

▷ On the Grassmann graph of linear codes

I. Cardinali, L. Giuzzi, M. Kwiatkowski, Finite Fields Appl. 75 (2021) 101895 doi:10.1016/j.ffa.2021.101895 (arxiv:2005.04402)

Let $\Gamma(n, k)$ be the Grassmann graph formed by the k-dimensional subspaces of a vector space of dimension n over a field $\mathbb{F}$ and, for $t \in \mathbb{N} \setminus \{0\}$, let $\Delta_t(n, k)$ be the subgraph of $\Gamma(n, k)$ formed by the set of linear $[n, k]$-codes having

minimum dual distance at least $t+1$. We show that if $|\mathbb{F}| \geq \binom{n}{t}$ then $\Delta_t(n,k)$ is connected and it is isometrically embedded in $\Gamma(n,k)$.

▷ Nearly all subspaces of a classical polar space arise from its universal embedding
I. Cardinali, L. Giuzzi, A. Pasini, Linear Algebra Appl. 627 (2021) 287-307 doi:10.1016/j.laa.2021.06.013 (arxiv:2010.07640)

Let Γ be an embeddable non-degenerate polar space of finite rank $n \geq 2$. Assuming that Γ admits the universal embedding (which is true for all embeddable polar spaces except grids of order at least 5 and certain generalized quadrangles defined over quaternion division rings), let $\varepsilon : \Gamma \to \mathrm{PG}(V)$ be the universal embedding of Γ. Let $\mathscr{S}$ be a subspace of Γ and suppose that $\mathscr{S}$, regarded as a polar space, has non-degenerate rank at least 2. We shall prove that $\mathscr{S}$ is the ε-preimage of a projective subspace of $\mathrm{PG}(V)$.

▷ Some hypersurfaces over finite fields, minimal codes and secret sharing schemes
A. Aguglia, M. Ceria, L. Giuzzi, Des. Codes. Cryptogr. 90 (2022) 1503-1519 doi:10.1007/s10623-022-01051-1 (arxiv:2105.14508)

Linear error-correcting codes can be used for constructing secret sharing schemes, however finding in general the access structures of these secret sharing schemes and, in particular, determining efficient access structures is difficult. Here we investigate the properties of certain algebraic hypersurfaces over finite fields, whose intersection numbers with any hyperplane only takes a few values. These varieties give rise to q-divisible linear codes with at most 5 weights. Furthermore, for q odd these codes turn out to be minimal and we characterize the access structures of the secret sharing schemes based on their dual codes. Indeed, we prove that the secret sharing schemes thus obtained are democratic that is, each participant belongs to the same number of minimal access sets.

▷ Characterizations of symplectic polar spaces
I. Cardinali, H. Cuypers, L. Giuzzi, A. Pasini, *to appear on* Adv. Geom. (arxiv:2205.14426)

A polar space $\mathscr{S}$ is said to be symplectic if it admits an embedding ε in a projective geometry $\mathrm{PG}(V)$ such that the ε-image $\varepsilon(\mathscr{S})$ of $\mathscr{S}$ is defined by an alternating form of V. In this paper we characterize symplectic polar spaces in terms of their incidence properties, with no mention of peculiar properties of their embeddings. This is relevant especially when $\mathscr{S}$ admits different (non isomorphic) embeddings, as it is the case (precisely) when $\mathscr{S}$ is defined over a field of characteristic 2.

▷ On the equivalence of certain quasi-Hermitian varieties
A. Aguglia, L. Giuzzi, J. Combin. Des. (2022) 1-15 doi:10.1002/jcd.21870 (arxiv:2108.04813)

In [A. Aguglia, A. Cossidente, G. Korchmaros, On quasi-Hermitian varieties, J. Comb. Des. 20 (2012), 433-447] new quasi-Hermitian varieties $\mathscr{M}_{\alpha,\beta}$ in $\mathrm{PG}(r,q^2)$ depending on a pair of parameters α,β from the underlying field $\mathrm{GF}(q^2)$ have been constructed. In the present paper we determine the projective equivalence classes of such varieties for $r=3$ and q odd.

▷ On the generation of some Lie-type geometries
I. Cardinali, L. Giuzzi, A. Pasini, J. Combin. Theory A 193 (2023) 105673, doi:10.1016/j.jcta.2022.105673 (arxiv:1912.03484)

Let $X_n(\mathbb{K})$ be a building of Coxeter type $X_n = A_n$ or $X_n = D_n$ defined over a given division ring $\mathbb{K}$ (a field when $X_n = D_n$). For a non-connected set J of nodes of the diagram X_n, let $\Gamma(\mathbb{K}) = \mathrm{Gr}_J(X_n(\mathbb{K}))$ be the J-Grassmannian of $X_n(\mathbb{K})$. We prove that $\Gamma(\mathbb{K})$ cannot be generated over any proper sub-division ring $\mathbb{K}_0$ of $\mathbb{K}$. As a consequence, the generating rank of $\Gamma(\mathbb{K})$ is infinite when $\mathbb{K}$ is not finitely generated. In particular, if $\mathbb{K}$ is the algebraic closure of a finite field of prime order then the generating rank of $\mathrm{Gr}_{1,n}(A_n(\mathbb{K}))$ is infinite, although its embedding rank is either $(n+1)^2-1$ or $(n+1)^2$.