# Curriculum vitae

Luca Giuzzi

9 giugno 2020

## 1 Dati personali


| | |
|---|---|
| Cognome: | Giuzzi |
| Nome: | Luca |
| Titolo: | Dr. (DPhil, Sussex) |
| Ruolo: | Professore Associato di Geometria |
| Data di Nascita: | 30 Settembre 1973 |
| Cittadinanza: | Italiana |
| Lingue conosciute: | Italiano (madre-lingua),<br>Inglese (molto buono). |
| Telefono: | +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 |
| Indirizzo (lavoro): | Dipartimento di Ingegneria Civile, Architettura,<br>Territorio, Ambiente e Matematica<br>Sezione di Matematica<br>Università degli studi di Brescia<br>via Branze 43<br>25123 Brescia<br>ITALIA |
| Indirizzo (residenza): | via Cesare Battisti 42<br>25018 Montichiari (BS)<br>ITALIA |


## 2 Titoli di studio

1. *Laurea in matematica* con una valutazione di 110 e lode/110 presso la Università Cattolica del Sacro Cuore; tesi dal titolo "Gruppi di Frobenius e strutture geometriche associate" sotto la supervisione del Prof. Silvia Pianta, 1996.
2. DPhil in Matematica presso la University of Sussex; tesi dal titolo "Hermitian varieties over finite fields" sotto la supervisione del Prof. James Hirschfeld, 2001.

## 3 Attività svolte

1. 1992-1996: Studente presso la Università Cattolica del Sacro Cuore.

2. 1996-1997: Amministratore di sistema presso l'Università Cattolica.

3. 1997-2000: Studente di dottorato presso University of Sussex (Brighton, UK).

4. 2000-2004: Assegnista di ricerca presso Università degli studi di Brescia.

5. Settembre 2002 – Maggio 2003: partecipazione al progetto "sviluppo di un crittosistema basato su curve ellittiche" (POP 342) in collaborazione con l'Università della Basilicata.

6. 14 Dicembre 2003: vincitore di concorso per Ricercatore Universitario presso il Politecnico di Bari sul settore scientifico–disciplinare MAT/03.

7. Gennaio 2005–Aprile 2008: Ricercatore Universitario presso il Politecnico di Bari.

8. Maggio 2008–Maggio 2018: Ricercatore Universitario presso l'Università degli Studi di Brescia.

9. Giugno 2018–ora: Professore Associato presso l'Università degli Studi di Brescia.

Luca Giuzzi è stato abilitato per il ruolo di *professore associato* in data 28 Marzo 2017.

Luca Giuzzi è *referee* per diverse riviste internazionali ISI. Inoltre è recensore per *MathSciNet* e *Zentralblatt MATH*.

## 4 Organizzazione di convegni

1. 2007: Parte del comitato organizzatore del "XVIII Congresso UMI", Bari.

2. 2008: Organizzatore della conferenza internazionale "Combinatorics 2008", Brescia.

3. 2017: Parte del comitato organizzatore della conferenza internazionale "Fq13", Gaeta.

4. 2017: Parte del comitato organizzatore della conferenza internazionale "HyGraDe", S. Alessio Siculo (Messina).

5. 2018: Parte del comitato organizzatore della conferenza internazionale "Combinatorics 2018", Arco (TN).

6. 2020: Parte del comitato organizzatore della conferenza internazionale "Combinatorics 2020", Mantova (MN).

## 5 Partecipazione a progetti PRIN finanziati

1. 2001: Strutture geometriche, combinatorica e loro applicazioni, in qualità di membro di unità locale;
2. 2003: Strutture geometriche, combinatoria e loro applicazioni, in qualità di membro di unità locale;
3. 2005: Grafi e Geometrie (2005018845_002), in qualità di membro di unità locale;
4. 2008: Strutture d'incidenza e combinatorie (2008BHF4AW_003), in qualità di membro di unità locale;
5. 2012: Strutture geometriche, combinatoria e loro applicazioni, (2012XZE22K_009) in qualità di Responsabile Scientifico dell'Unità Locale di ricerca di Brescia.

## 6 Partecipazione a progetti Europei

1. 2013: Partecipazione al progetto "COST Action IC1104: Random Network Coding and Designs over GF($q$)"

## 7 Attività didattica

In quanto titolare di corsi universitari per affidamento, ai sensi dell'art. 1, comma 11, della Legge 4.11.05 n. 230 è stato attribuito al Prof. Giuzzi il titolo di *professore aggregato* a partire dal Settembre 2006 al Giugno 2018. Dal 2018 è *Professore Associato in Geometria*.

1. 1998–1999: esercitatore per il corso di Matematica discreta presso la University of Sussex.
2. 1999–2000: esercitatore per i corsi di Matematica Discreta e Teoria dei Gruppi presso la University of Sussex.
3. 2000–2001: mini-corso (10 ore) sulla crittografia presso la Università Cattolica del Sacro Cuore.
4. 2001–2002: mini-corso su "Crittografia: dal DES all'AES" presso l'Università di Brescia.
5. 2003-2004: seminari per la durata di 10 ore nell'ambito del corso di Matematica Discreta, presso l'Università di Brescia.
6. 2004–2005: titolare per affidamento del corso di "Geometria Superiore 2" per il secondo anno della laurea specialistica in Matematica presso l'Università Cattolica del Sacro Cuore.
7. 2004–2005: assistenza esami/didattica integrativa per il corso di Geometria e Algebra di Ingegneria Meccanica A, Ingegneria Gestionale A e B presso la prima facoltà del Politecnico di Bari.
8. Settembre 2005: corso di azzeramento presso la prima facoltà del Politecnico di Bari.
9. 2005–2006: corso di esercitazioni di Geometria e Algebra per i corsi di Ingegneria Meccanica A, Ingegneria Gestionale A, Ingegneria Gestionale B, presso la prima facoltà del Politecnico di Bari.
10. 2006–2007: titolare per affidamento del corso di "Geometria e Algebra" (6 crediti) per il primo anno della laurea in Ingegneria Meccanica (corso A), presso il Politecnico di Bari; corso di esercitazioni per il corso di "Geometria e Algebra" per Ingegneria delle Telecomunicazioni presso il Politecnico di Bari.

11. 2007–2008: titolare per affidamento del corso di "Geometria e Algebra" (6 crediti) per il primo anno della laurea in Ingegneria Meccanica (corso A), presso il Politecnico di Bari; corso di esercitazioni per il corso di "Geometria e Algebra" per Ingegneria delle Telecomunicazioni presso il Politecnico di Bari.
12. 2007: seminari (3 ore) relativi la teoria dei codici presso l'Università degli studi di Brescia, nell'ambito del progetto n. 411498 del Fondo Sociale Europeo, Ob. 3 Mis. C3 (2006), 414809, no. 671794 "Corso di alta formazione nell'ambito di dottorati afferenti al settore dell'Ingegneria dell'informazione".
13. 2008: correlatore per tesi di primo e secondo livello in Matematica presso l'Università Cattolica di Brescia.
14. 2008–2010: titolare per affidamento del corso di "Complementi di Algebra e Geometria" per il primo anno della laurea Specialistica in Ingegneria Civile presso l'Università degli Studi di Brescia.
15. 2010–2011: titolare per affidamento del corso di "Algebra per Codici e Crittografia" per corsi di laurea triennale e magistrale presso l'Università degli Studi di Brescia.
16. 2011-2012: titolare per affidamento dei corsi di
    - "Algebra per Codici e Crittografia", Università degli Studi di Brescia;
    - "Geometria combinatorica" (Combinatorial geometry), Università Cattolica del S. Cuore (BS).
17. 2012-2018: titolare per affidamento dei corsi di
    - "Algebra per Codici e Crittografia", Università degli Studi di Brescia;
    - "Algebra e Geometria", Università degli studi di Brescia.
18. 2018-ora: professore titolare dei corsi di
    - "Algebra per Codici e Crittografia" (6 CFU), Università degli Studi di Brescia;
    - "Algebra e Geometria" (9 CFU), Università degli studi di Brescia.

Dal 2012 è stato relatore di numerose Tesi di Laurea di Primo Livello in Ingegneria dell'Informazione, preminentemente su tematiche di crittografia: *La cifratura omomorfica* (2012), *Sistemi crittografici per SMS* (2012), *Sistemi di voto elettronico* (2013), *Metodi steganografici per documenti PDF* (2013), *Il crittosistema KeeLoq* (2014), *Crittografia distribuita* (2014), *Cloud computing e privacy: tecniche di verifica dei servizi di data storage* (2014), *Analisi di un sistema di voto elettronico* (2015), *Crittosistemi elettromeccanici: macchine cifranti nella seconda guerra mondiale* (2015), *Verifica di integrità per il Cloud storage* (2016), *Geolocalizzazione occulta* (2016), *Game theory and its applications* (2017, Ing. Gestionale), *Steganografia e watermarking per files JPG* (2017), *The PURPLE cipher machine* (2018), *La crittoanalisi di Enigma: implementare la "bomba"* (2018), *Quantum computing: la simulazione dell'algoritmo di Shor* (2018), *Programmare la BlockChain: sistemi di voto elettronico* (2018), *Sicurezza informatica e ransomware: il caso Wannacry* (2019), *Crittografia omomorfica con HELIB* (2019), *Crittografia per messaggistica istantanea: il protocollo Signal* (2019), *Network coding and rank distance codes* (2019, Magistrale), *Autenticazione delle reti wireless: da WEP a WPA3* (2019), *Reti neurali e crittografia* (2019), *Blockchain private e applicazioni distribuite con hyperledger* (2020), *Macchine virtuali per crittovalute: bitcoin ed ethereum* (2020), *Steganografia TCP/IP* (2020), *Sistemi di Internet Voting* (2020), *Algoritmi su reticoli per crittografia post-quantum* (2020), *Macchine cifranti: la SZ-40* (2020), *Sicurezza dei sistemi di pagamento tramite app* (2020), *Trattamento delle informazioni in ambito ospedaliero e protocolli di sicurezza* (2020), *Sicurezza per le reti in-vehicle* (2020), *Criptovalute a confronto: Bitcoin e Libra* (2020), *Crittosistemi Post-Quantum: NTRU e sue varianti* (2020), *Watermarking per immagini* (2020), *Post-Quantum digital signatures* (2020).

## 8 Lavori accettati

1. 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.

2. 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.

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

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

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

6. 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.

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

8. 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).

9. 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).

10. 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).

11. 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).

12. 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).

13. 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).

14. 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).

15. 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).

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

17. 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).

18. 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).

19. 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).

20. 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).

21. 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).

22. 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).

23. 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.

24. 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).

25. 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).

26. 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).

27. 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).

28. 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).

29. 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).

30. 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).

31. 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).

32. 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).

33. 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).

34. 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).

## 9 Preprints

1. A. Aguglia, L. Giuzzi, M. Homma, "On Hermitian varieties in PG$(6, q^2)$, (arxiv:2006.04099).
2. I. Cardinali, L. Giuzzi, M. Kwiatkowski, "On the Grassmann Graph of Linear Codes", (arxiv:2005.04402).
3. I. Cardinali, L. Giuzzi, A. Pasini, "Generation of $J$-Grassmannians of buildings of type $A_n$ and $D_n$ with $J$ a non-connected set of types", (arxiv:1912.03484).
4. I. Cardinali, L. Giuzzi, A. Pasini, "The generating rank of a polar Grassmannian", (arxiv:1906.10560).
5. L. Giuzzi, A. Sonnino, "Alcune note introduttive sulla crittografia", Quaderno del seminario matematico di Brescia n. 01/2006.
6. L. Giuzzi, "Looking for ovoids of the Hermitian surface: a computational approach", Quaderno del seminario matematico di Brescia n. 33/2002, (arxiv:1210.2600).
7. L. Giuzzi, "Intersections of Hermitian surfaces/2: matrices", Quaderno del seminario matematico di Brescia n. 14/2001.
8. L. Giuzzi, "Intersections of Hermitian surfaces/1: configurations", Quaderno del seminario matematico di Brescia n. 11/2001.
9. L. Giuzzi, "Size of Hermitian intersections", Quaderno del seminario matematico di Brescia n. 07/2001.
10. 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.

## 10 Monografie

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

## 11 Brevetti

1. L. Giuzzi, G. Korchmàros, A. Sonnino, "Perfezionamenti nella crittografia a chiave pubblica basata su curve ellittiche", brevetto numero 0001379714 conferito in data 30 Agosto 2010.

## 12 Proceedings

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).

## 13 Altri lavori a stampa

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, relatore Prof. S. Pianta.

## 14 Riconoscimenti, borse di studio e finanziamenti

1. Maggio 1997: assegno di perfezionamento all'estero da parte dell'Università Cattolica.
2. Luglio 1997: borsa di studio per dottorato all'estero assegnata dallo INDAM; tale borsa di studio è stata rinnovata per gli anni 1998–1999 e 1999–2000.
3. 1997-2000: riconoscimento da parte dell'EPSRC con pagamento della retta universitaria per il corso di dottorato.
4. Giugno 2000: borsa di ricerca nell'ambito di "Progetto e realizzazione di un crittosistema per comunicazioni", POP-FESR 1994/99, Università della Basilicata.
5. Settembre 2000: assegno di ricerca presso l'Università degli studi di Brescia, rinnovato sino al 29 Dicembre 2004.
6. 2001: Dispensato dal servizio di Leva sensi dell'Art. 7(d) DLG 504/97 in quanto "Cittadino impegnato, con meriti particolari, sul piano nazionale o internazionale in carriere scientifiche, artistiche, culturali."
7. 2015, "Incentivo una tantum anno 2011" (per attivita' degli anni 2008-2011).
8. 2017, "Incentivo una tantum anno 2013" (per attivita' degli anni 2011-2013)
9. 2017: Ammesso al finanziamento per le Attività di Base della Ricerca (FABR) cui all'avviso pubblico ANVUR prot. 20/2017 del 15 Giugno 2017.

## 15 Selezione di scuole e workshops

1. Luglio 1995: "Summer school on combinatorics and finite geometry", Potenza.
2. Luglio 1996 "Summer school Giuseppe Tallini on finite geometry", Brescia.
3. Agosto 1996, "Scuola di Matematica Interuniversitaria", Perugia.
4. Settembre 1997, "Summer school on finite geometry", Potenza.
5. Aprile 1998, Corso intensivo "Galois Geometry and Generalised Polygons", Ghent.
6. Luglio 1998, "Advanced school on Combinatorial Geometry", Cortona;
7. Agosto 1998, NATO Advanced Study Institute "Difference sets, sequences and their correlation properties", Bad Winsheim.
8. Settembre 1998, "Summer school Giuseppe Tallini on finite geometry", Brescia.
9. Novembre 1998, Workshop "SUNCAGe'98", Caserta.

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

## 16 Comunicazioni

1. 6 Novembre 1997, "Spazi co–Minkowski e loro struttura di riflessione", GNSAGA national meeting, Perugia (IT).
2. 19 Giugno 1998, "Co-Minkowski spaces and their reflection structure", Combinatorics '98, Palermo (IT).
3. 31 Maggio 2000, "Intersection numbers for Hermitian varieties", Combinatorics 2000, Gaeta (IT).
4. 19 Luglio 2000, "Groups stabilising the intersection of two classical unitals", Fourth Isle of Thorns conference of finite geometries, Isle of Thorns (UK).
5. 5 Luglio 2001, "A short characterisation of classical unitals", 18th British Combinatorial Conference, Brighton.

6. 8 Giugno 2002, "Ovoids of the Hermitian surface", Combinatorics 2002, Maratea (IT).
7. 3 Ottobre 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 Giugno 2006, "LDPC Codes from Projective Spaces", Combinatorics 2006, Ischia (IT).
9. 30 Gennaio 2010, "Geometria e codici", giornata in onore del Prof. M. Marchi, in occasione del suo 70mo compleanno.
10. 29 Giugno 2010, "On samplings of graphs", Combinatorics 2010, Verbania (IT)
11. 12 Luglio 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 Settembre 2012, "Caps and codes from Polar Grassmannians", Combinatorics 2012, Perugia (IT)
13. 19 Settembre 2013, "Linear codes from orthogonal Grassmannians", Conference on Random network codes and Designs, Ghent (BE).
14. 5 Giugno 2014, "On Line Polar Grassmann Codes", Combinatorics 2014, Gaeta (IT).
15. 19 Giugno 2014, "Linear Polar Grassmann Codes", Algebra, codes and Networks, Bordeaux (FR).
16. 18 Settembre 2014, "Intersection of Hermitian Surfaces and quadrics", Finite Geometries — Fourth IRSEE conference, Kloster Irsee (DE).
17. 16 Marzo 2015, "Polar Grassmann codes — Part II", ALCOMA15, Kloster Banz (DE).
18. 19 Giugno 2015, "Polar Grassmannians and their Codes", MEGA2015, Trento (IT).
19. 3 Giugno 2016, "Implementing Polar Graßmann Codes", Combinatorics 2016, Maratea (IT).
20. Giugno 2017, "Hermitian Line Polar Graßmann Codes", Fq13, Gaeta (IT).
21. Settembre 2017, "Transparent embeddings of point-line geometries", Fifth Irsee Conference, Irsee (DE).

## 17 Seminari

Tutti i seminari descritti in questo paragrafo sono stati su invito delle istituzioni ospitanti.

1. Giugno 1997, "Kinematic spaces derived from Frobenius Groups", School of Mathematical Sciences, University of Sussex.
2. 23 e 24 Settembre 1998, "Crittografia e geometrie finite (I e II)", dipartimento di Matematica, Università Cattolica del Sacro Cuore, Brescia.
3. 16 Ottobre 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, seminario pubblico su "Fiducia, informazione e riservatezza: la teoria delle *scritture segrete* e le sue implicazioni legali", Università Cattolica del Sacro Cuore, Brescia.
6. 23 Maggio 2001, "Intersezione di varietà Hermitiane", Università di Brescia.
7. 5 Dicembre 2001, "Varietà Hermitiane su campi finiti: perchè?", Università Cattolica del Sacro Cuore, Brescia.
8. 10 Aprile 2002, "Calotte e ovoidi della superficie Hermitiana: un approccio computazionale", Università di Brescia.
9. 11 Luglio 2002, "Una introduzione alla crittografia moderna: da RSA ad AES", Summer School "Giuseppe Tallini" 2002, Brescia.
10. 5 Febbraio 2003, "Una introduzione alla teoria dei codici" Università Cattolica del Sacro Cuore, Brescia.
11. 12 Febbraio 2003, "Dai Codici ai Disegni", Università Cattolica del Sacro Cuore, Brescia.
12. 6 Novembre 2003, "Incidence configurations in the Hermitian surface", Giornate di Geometria, Università Cattolica del Sacro Cuore, Brescia.
13. 20 Novembre 2003, "Matematica più segretezza", Museo delle Scienze, Brescia.
14. 4 Maggio 2004, "Geometrie finite e crittografia", Politecnico di Bari.
15. 6 Maggio 2004, "Campi finiti in C++", Dipartimento di Matematica, Università Federico II, Napoli.
16. 9 Settembre 2005, "A defense of cryptography", Università della Basilicata.
17. 29 Maggio e 31 Maggio 2006, "Introduzione alla decodifica algebrica di codici ciclici", Facoltà di Ingegneria, Università di Brescia.
18. 25 Ottobre 2006, "Sicurezza, confidenzialità e segretezza: diversi aspetti della crittografia", Dipartimento di Matematica, Università di Bari.
19. 21 Novembre 2006, "Codici di Reed–Solomon", Facoltà di Ingegneria, Università di Brescia.
20. 23 Novembre 2006, "Crittografia per la (in)sicurezza", Facoltà di Ingegneria, Università di Brescia.
21. 4 e 6 Dicembre 2006, "Usi della crittografia: dalla segretezza alla sicurezza", Facoltà di Economia di Bari.
22. 5 Dicembre 2008, "Curve ellittiche: teoria", Università Cattolica, Brescia.
23. 13 Febbraio 2009, "Curve ellittiche: pratica", Università Cattolica, Brescia.
24. 8 Aprile 2009, "Codici BCH non binari", Università Federico II, Napoli.
25. 30 Gennaio 2010, "Geometry and codes", WorkShop in onore of M. Marchi, Università Cattolica, Brescia.
26. 29 Ottobre 2010, "La matematica dei segreti", Università Cattolica, Brescia.
27. Dal 15 al 21 Maggio 2011 L. Giuzzi è stato ospite del dipartimento di Matematica dell'Università di Gent (BE).
28. 15 Marzo 2012, "Non–linear codes", Dipartimento di Matematica, Università Federico II, Napoli.

29. 24 Aprile 2012, “Algebraic and geometric methods in cryptography”, Dipartimento di Matematica, Politecnico di Milano.
30. 21 Gennaio 2014, “Strutture geometriche, combinatorica ed applicazioni”, DICATAM, Università di Brescia.
31. 28 Maggio 2019, “Grassmanniane Polari”, Università di Siena.

## 18 Descrizione degli interessi di ricerca

1. Geometrie di incidenza.
2. Teoria dei codici e crittografia.
3. Geometrie finite e varietà su campi finiti.
4. Disegni su grafi e loro proprietà.

## 19 Competenze informatiche

1. Conoscenza approfondita del sistema operativo Linux.
2. Esperienza sistemistica con Solaris (2.5–2.8) e Digital Unix v4.0.
3. Buona conoscenza di C, C++ e python.
4. Buona conoscenza di HTML e XHTML nonché CSS.
5. Esperienza con perl e PHP.
6. Conoscenza pratica di diversi sistemi di computer algebra, fra cui GAP, Maxima, Axiom, Singular and Pari/GP.

## 20 Descrizione di alcune pubblicazioni

▷ Hermitian varieties over finite fields

L. Giuzzi, University of Sussex (2000)

Nella tesi di dottorato "Hermitian varieties over finite fields" si sono investigate alcune delle proprietà delle configurazioni che nascono dall'intersezione di varietà Hermitiane in spazi proiettivi finiti.

In particolare, si sono ottenuti i seguenti risultati:

1. si è determinato il gruppo totale delle collinezioni lineari che stabilizzano l'intersezione di due curve Hermitiane e si è provato che se due intersezioni determinano la medesima struttura di incidenza punto–linea, allora esse sono proiettivamente equivalenti;

2. si è fornita una nuova dimostrazione della caratterizzazione dell' *unital* classico di $\mathrm{PG}(2, q^2)$ come l'*unital* stabilizzato da un gruppo ciclico di collineazioni di ordine $q^2 - q + 1$;

3. si sono descritte le configurazioni punto–linea–piano che nascono dall'intersezione di due superfici Hermitiane;

4. si sono calcolate le liste delle possibili cardinalità di intersezione per due qualsiasi varietà Hermitiane in $\mathrm{PG}(n, q^2)$.

▷ Codici Correttori

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

Il testo è finalizzato a fornire un'introduzione generale alla teoria algebrica dei codici ed è destinato a studenti del terzo anno di un corso Laurea di primo livello in Matematica, Fisica o Ingegneria, oppure del primo/secondo anno di Laurea Specialistica.

Il piano dell'opera è il seguente.

1. Nei primi due capitoli si richiamano alcune nozioni di teoria matematica della comunicazione; tale teoria fornisce la giustificazione delle tecniche di correzione di errore che sono l'oggetto del resto del testo.

2. Nel Capitolo 3 si introducono le nozioni di codice a blocchi di correzione, codifica e decodifica di un messaggio, nonché di equivalenza fra codici.

3. I capitoli dal 4 al 15 costituiscono il cuore del lavoro: in essi vengono studiate numerose famiglie di codici lineari e si mostra il loro impiego e quali proprietà debbano sempre essere soddisfatte.

4. Il Capitolo 4 è finalizzato ad introdurre i codici lineari, visti come spazi vettoriali, e a presentarne le proprietà generali;

5. Oggetto dei capitoli 5 e 6 sono un tipo particolare di codici lineari: i codici ciclici. Tali codici si possono descrivere in modo estremamente conciso e si rivelano particolarmente utili per correggere alcune tipologie di errore, quali gli errori concentrati. Questa classe di errore è studiata nel dettaglio nel Capitolo 7.

6. Nel Capitolo 8 si definisce la costruzione BCH e si studiano i codici da essa derivati. Uno degli aspetti più importanti di tale costruzione è che consente di fissare *a priori* il numero di errori che un codice deve poter correggere.

7. I codici di Reed–Solomon, oggetto del Capitolo 9, costituiscono forse la più importante famiglia di codici lineari a blocchi: sono infatti implementati in svariati dispositivi di comunicazione digitale. Fra i motivi del loro successo vi è l'esistenza di eccellenti algoritmi di correzione specifici, ma anche la possibilità di utilizzarli per correggere errori di cui si conosce la posizione ma non l'entità. Metodologie per affrontare quest'ultimo problema sono introdotte nel Capitolo 10.

8. Nel Capitolo 11 si presenta come sia possibile costruire dei codici a partire da strutture di tipo geometrico–combinatorico; tali costruzioni sono utilizzate anche nel Capitolo 12 per costruire i codici sporadici di Golay e mostrare che sono perfetti.

9. I codici di Reed–Müller sono una possibile generalizzazione dei codici di Reed–Solomon; nel Capitolo 13 mostriamo come costruirli e, nel caso binario, ne deriviamo alcune proprietà.

10. Non sempre è facile ottenere direttamente un codice che abbia i parametri richiesti per un ben definito problema pratico. Tecniche per determinare codici con il comportamento desiderato, a partire da codici altrimenti noti, sono presentate nel Capitolo 14.

11. Nel capitolo conclusivo di questa parte del libro, il 15, si presentano alcune limitazioni assolute al comportamento di un codice e si dimostra che, quantomeno a livello teorico, è sempre possibile costruire dei codici con il miglior comportamento possibile.

12. I capitoli della terza parte del volume (dal 16 al 18) sono destinati a fornire un'idea generale su alcune classi di codici che sono correntemente oggetto di intensa ricerca. Tali capitoli non vogliono essere esaustivi ma semplicemente stimolare il lettore interessato ad approfondire l'argomento. Le classi considerate sono quella dei codici Algebrico–Geometrici (Capitolo 16), dei codici LDPC (Capitolo 17) e quella dei codici convoluzionali (Capitolo 18).

13. Concludono il testo due appendici: una (Appendice A) sui campi finiti, l'altra sulle curve algebriche (Appendice B).

I capitoli dal 2 al 14 sono corredati di esercizi svolti. Nello svolgimento degli stessi si è cercato, ove opportuno, di mostrare come i problemi possano essere impostati utilizzando il sistema di *computer algebra* GAP. Tale sistema è liberamente disponibile in rete (si veda la bibliografia per l'indirizzo) ed è finalizzato allo studio di strutture algebriche finite.

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

B. Kestenband ha dimostrato nel 1981 che esistono solamente sette possibili configurazioni a due a due non isomorfe per l'intersezione di due curve Hermitiane (Unitals classici) nel piano proiettivo desarguesiano $\mathrm{PG}(2, q)$, $q$ quadrato. Tale classificazione è basata sullo studio dei polinomi minimi delle matrici associate con le curve e conduce a risultati di natura puramente combinatoria. In questo lavoro si completa la classificazione proiettiva di tali configurazioni e si dimostra che ognuna delle classi di Kestenband consiste di intersezioni proiettivamente equivalenti. Inoltre, si fornisce una classificazione completa dei gruppi di collineazioni lineari che conservano una intersezione Hermitiana.

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

In questo lavoro si costruisce una famiglia infinita di K-loops a partire dalla struttura di riflessione di un piano di tipo co-Minkowski. Successivamente, viene studiata la struttura del K-loop così ottenuto sotto l'ipotesi aggiuntiva che il piano co-Minkowski sia definito su di un campo $K$ in cui 2 è un quadrato. Si dimostra che questo loop è sempre fibrato in sottogruppi ed è possibile descrivere la struttura dei suoi

centralizzanti in modo geometrico. L'ultima parte dell'articolo è dedicata alla analisi della azione del gruppo di struttura del loop sulle linee del cono quadratico del piano co-Minkowski.

▷ A Characterisation of Classical Unitals

L. Giuzzi, J. Geom., 74: 86–89 (2002).

Un *unital* $\mathcal{U}$ di PG$(2,q)$ è un insieme di $q\sqrt{q}+1$ punti tali che ogni linea di PG$(2,q)$ interseca $U$ in $1$ oppure $\sqrt{q}+1$ punti. I punti assoluti di una polarità unitaria di PG$(2,q)$ formano un *unital*, detto *unital classico*. In questo lavoro viene fornita una breve dimostrazione della seguente proprietà: "Un unital di PG$(2,q)$ è classico se e solo se esso è conservato da un gruppo ciclico di collineazioni lineari di ordine $q-\sqrt{q}+1$.

▷ Ovoids of the Hermitian Surface in Odd Characteristic

L. Giuzzi, G. Korchmáros, Adv. Geom., Special Issue (2003), S49–S58.

In questo lavoro viene costruito un nuovo ovoide dello spazio polare indotto dalla superficie Hermitiana di PG$(3,q)$ con $q>25$ dispari. Il gruppo di automorfismi $\Gamma$ di tale ovoide contiene un sottogruppo normale ciclico $\Phi$ di ordine $\frac{1}{2}(\sqrt{q}+1)$ tale che $\Gamma/\Phi \simeq PGL(2,q)$. Inoltre si verifica che $\Gamma$ possiede tre orbite sull'ovoide, una di lunghezza $\sqrt{q}+1$ e due di lunghezza $\frac{1}{2}\sqrt{q}(\sqrt{q}-1)(\sqrt{q}+1)$.

▷ On the Intersection of Hermitian Surfaces

L. Giuzzi, J. Geom., 85: 49–60 (2006).

In questo articolo si fornisce una descrizione delle possibili configurazioni di punti che nascono dall'intersezione di due superficie Hermitiane nello spazio proiettivo PG$(3,q^2)$, sotto l'ipotesi che il sistema lineare generato da tali superficie contenga almeno una varietà degenere. Inoltre, si fornisce un elenco di tutte le possibili cardinalità che l'intersezione di due ipersuperficie Hermitiane può assumere in PG$(n,q^2)$.

▷ A Geometric Construction for Some Ovoids of the Hermitian Surface

L. Giuzzi, Results Math. 49: 81–88 (2006).

Un generatore della superficie Hermitiana non degenere $\mathcal{H}(3,q^2)$ è una retta dello spazio proiettivo PG$(3,q^2)$ completamente contenuta nella superficie. Un *ovoide* di $\mathcal{H}(3,q^2)$ è un insieme di $q^3+1$ punti che incontra ogni generatore della superficie stessa in esattamente un punto. L'intersezione di $\mathcal{H}(3,q^2)$ con un piano non tangente è un ovoide, il cosiddetto *ovoide classico* della superficie Hermitiana. L'esistenza di ovoidi non classici è stata dimostrata per la prima volta nel 1994. Un medodo per ottenere alcuni ovoidi non classici consiste nell'applicare una procedura detta derivazione a partire dall'ovoide classico. Nel presente articolo si descrive in termini geometrici un ovoide non classico e si dimostra che esso è derivabile.

▷ Orthogonal Arrays from Hermitian Varieties

A. Aguglia, L. Giuzzi, Innov. Incidence Geom. 5: 129–144 (2007).

Una matrice $A$, di dimensioni $k\times N$, contenente $q$ simboli e con la proprietà che ogni suo minore di dimensione $t\times N$ contenga ogni colonna $t\times 1$ esattamente $\mu=N/q^t$ volte è detto *array ortogonale* di forza $t$ e indice $\mu$. Gli *array ortogonali* sono un importante strumento per la costruzione di esperimenti statistici e sono strettamente legati alle proprietà dei disegni risolubili. Nel presente articolo si è costruito un array ortogonale *semplice* (cioè privo di colonne ripetute) a partire da opportune varietà Hermitiane e si è mostrato come esso sia strettamente legato ad un modello non classico dello spazio affine di dimensione $(2n-1)$.

▷ Construction of a 3–dimensional MDS Code

A. Aguglia, L. Giuzzi, Contrib. Discrete Math. 3 (1), 39–46 (2007).

In questo articolo si mostra come costruire un $[N, 3, N-2]$–codice MDS $q$–ario di lunghezza al più $q+1$ per $q$ dispari e $q+2$ per $q$ pari. Si fornisce inoltre per tale codice una descrizione puramente geometrica della procedura di correzione e decodifica.

▷ An Algorithm for Constructing some Maximal Arcs in PG$(2, q^2)$

A. Aguglia, L. Giuzzi, Results Math. 52 no. 1–2: 17–33 (2008).

Un arco massimale di ordine $n$ del piano proiettivo PG$(2, q)$ è un insieme non vuoto di punti $A$ tale che ogni retta del piano incontri $A$ in $0$ oppure in $n$ punti. È stato dimostrato che quando $q$ è dispari non esistono archi massimali non banali; nel caso $q$ pari, invece, sono note diverse costruzioni. Al fine di investigare al meglio le proprietà di tali costruzioni, è opportuno implementare le strutture mediante l'utilizzo di sistemi di *computer algebra*. Nel presente articolo si mostra come costruire degli archi massimali in PG$(2, q^2)$ utilizzando il programma GAP.

▷ Algebraic Curves and Maximal Arcs

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

In questo lavoro si fornisce una limitazione inferiore sul grado minimo di una curva algebrica piana che contenga tutti i punti di un insieme "grande" di punti $K$ del piano proiettivo Desarguesiano. Si ottengono inoltre alcune limitazioni specifiche per il caso in cui $K$ sia un arco massimale. Questi risultati sono poi applicati alla caratterizzazione degli archi massimali di grado $4$ ricoperti da una curva di grado minimo (7).

▷ 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).

Una ovale $\Omega$ in un piano proiettivo finito $\Pi$ di ordine $q$ è un insieme di $q+1$ punti a due a due non allineati. In generale, il problema di determinare quali piani non Desarguesiani posseggano ovali appare di difficile risoluzione ed è correntemente aperto nel caso generale. Ad esempio, sono noti alcuni piani proiettivi finiti di ordine $16$ privi di ovali, mentre altri ne sono dotati.

Una tecnica che si è rivelata particolarmente fruttuosa per costruire ovali in piani non Desarguesiani è quella delle "ovali ereditate", dovuta a G. Korchmáros. Essa funziona bene nel caso dei piani di Moulton di ordine dispari. Nel presente lavoro si dimostra come i piani di Moulton di ordine pari non possano contenere alcuna ovale (o iperovale) ereditata da quelle classiche.

▷ LDPC Codes from Singer Cycles

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

L'obiettivo principale della teoria dei codici è quello di costruire sistemi efficienti per sfruttare appieno la capacità di un canale di comunicazione. I codici con matrice di controllo di parità a bassa densità sono stati introdotti da Gallager nel 1962 e ignorati per lungo tempo; nel 1999, MacKey ha mostrato come essi possano essere applicati a canali digitali ad alta velocità e come sia possibile decodificarli in modo estremamente efficiente. In generale, il problema di costruire codici LDPC facilmente codificabili si è rivelato tutt'altro che banale. Nel presente articolo si mostra come sia possibile costruire delle matrici per codici LDPC in modo efficiente a partire dalle orbite di sottospazi dello spazio proiettivo finito $PG(n-1, q)$ sotto l'azione di un ciclo di Singer.

▷ Construction of Unitals in Desarguesian Planes
A. Aguglia, L. Giuzzi, G. Korchmáros, Discrete Math. 310 (22): 3162–3167 (2010).

Uno *unital* in un piano proiettivo finito di ordine $q^2$ è un insieme di $q^3+1$ punti intersecato da ogni retta del piano in 1 oppure $q+1$ punti distinti. L'esempio classico di unital nel piano Desarguesiano PG$(2,q^2)$ è dato dai punti assoluti di una polarità unitaria.

In questo lavoro si introduce una nuova costruzione per unitals non classici di tipo Buekenhout-Metz (BM) o Buekenhout-Tits (BT). In particolare, si descrive un modello non-standard di $PG(2,q^2)$ in cui i punti di una curva Hermitiana vengono a rappresentare quelli di un unital di tipo BM oppure BT. Tale risultato consente inoltre di caratterizzare i codici associati ad unitals di tipo BM e BT.

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

Siano $\Gamma$ e $\Delta$ due grafi con $\Gamma \leq \Delta$. Un $\Delta(\Gamma)$-disegno completo è l'insieme di tutti i sottografi di $\Delta$ isomorfi a $\Gamma$. Siano ora $\Gamma' \leq \Gamma$ due grafi. In questo lavoro si introduce la nozione di *sampling* di un $\Gamma$-disegno $\mathfrak{B}$ in un $\Gamma'$-disegno $\mathfrak{B}'$ quale funzione suriettiva $\xi : \mathfrak{B} \to \mathfrak{B}'$ che assegna ad ogni blocco di $\mathfrak{B}$ un suo sottografo in $\mathfrak{B}'$. Una sampling è detta regolare quando il numero di preimmagini di un elemento di $\mathfrak{B}'$ secondo $\xi$ è costante. Si verifica che tale nozione è strettamente legata a quelle, diffusamente studiate in letteratura, di embedding e di nesting. Nel lavoro in oggetto si dimostra come la condizione naturale necessaria per l'esistenza di una sampling sia in effetti anche sufficiente. Inoltre vengono fornite alcune costruzioni esplicite e si suggeriscono possibili generalizzazioni.

▷ Unitals in PG$(2,q^2)$ with a large 2–point Stabiliser
L. Giuzzi, G. Korchmáros, Discrete Math. 312 (3): 532–535 (2012).

Sia $\mathcal{U}$ uno unital nel piano proiettivo Desarguesiano PG$(2,q^2)$. In questo lavoro si dimostra che se $\mathcal{U}$ possiede due punti distinti $P,Q$ tali che lo stabilizzante di $P$ e $Q$ nel gruppo di tutte le collineazioni che fissano $\mathcal{U}$ ha ordine $q^2-1$, allora $\mathcal{U}$ è classico, ovvero è il luogo dei punti assoluti di una polarità unitaria.

▷ Down–linking $(K_v,\Gamma)$-designs to $P_3$-designs
A. Benini, L. Giuzzi, A. Pasotti, Util. Math. 90: 3–21 (2013).

Sia $\Gamma'$ un sottografo di $\Gamma$. Un $(K_v,\Gamma)$-disegno è una decomposizione dell'insieme degli spigoli di $K_v$ in sottografi tutti isomorfi a $\Gamma$. In questo lavoro viene introdotta la nozione di *down-link* fra un $(K_v,\Gamma)$-disegno $\mathfrak{B}$ e un $(K_n,\Gamma')$-disegno $\mathfrak{B}'$. Esso è una funzione $\xi : \mathfrak{B} \to \mathfrak{B}'$ che associa ad ogni blocco di $B$ un suo sottografo. Tale nuovo concetto risulta legato alle nozioni classiche di metamorfosi (e metamorfosi generalizzata) nonché di embedding. In particolare, in questo lavoro si dimostra che ogni $(K_v,\Gamma)$-disegno può essere collegato mediante un down-link con un $(K_n,\Gamma')$-disegno per ogni $\Gamma' \leq \Gamma$, a patto che $n$ sia abbastanza grande e alcune ulteriori condizioni naturali siano soddisfatte. Si verifica inoltre che è sempre possibile costruire un down-link da un $(K_v,\Gamma)$-disegno in un $(K_n,P_3)$-disegno con $v \leq v+3$, ove $P_3$ denota un cammino su 3 vertici. Tale limitazione viene poi migliorata nel caso di svariate classi di grafi fornendo costruzioni esplicite.

▷ New Results on Path–decompositions and their Down-links
A. Benini, L. Giuzzi, A. Pasotti, Util. Math. 90: 369-382 (2013).

In questo lavoro si studia l'esistenza di down–links di disegni di tipo $(K_v,\Gamma)$ in $(K_n,P_4)$–disegni, con particolare attenzione ai casi dei cammini $\Gamma = P_k$ e dei cicli $\Gamma = C_k$. Le condizioni generali di esistenza e le limitazioni sullo spettro sono poi analizzate in dettaglio nei casi particolari $\Gamma = P_5$ e $\Gamma = C_4$ ove si forniscono costruzioni esplicite.

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

In questo lavoro si considerano codici correttori di errore legati alla della varietà $\mathcal{V}_{r,t}$, immagine sotto la mappa di Grassmann di una $(t-1)$-fibrazione desarguesiana di PG$(rt-1,q)$. In tale modo vengono determinate numerose famiglie di codici constaciclici, i cui parametri sono calcolati. Si fornisce inoltre una caratterizzazione delle parole di peso minimo.

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

In questo lavoro si studiano codici correttori di errore e calotte proiettive collegati all'immersione di Grassmann $\varepsilon_k^{gr}$ di una Grassmanniana ortogonale $\Delta_k$. Più nello specifico, si stimano i parametri dei codici associati al sistema proiettivo dei punti di $\varepsilon_k^{gr}(\Delta)$. Si introduce inoltre la nozione di $m$–calotta polare: un insieme di $m$ punti di $\Delta_k$ caratterizzato dall'incontrare ogni retta in al più 2 elementi e si dimostra che l'immagine sotto l'immersione $\varepsilon_k^{gr}$ di una calotta polare è una calotta proiettiva. Infine, si determinano alcune speciali calotte polari associate a matrici di Hadamard.

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

In questo articolo si determina la lista delle possibili intersezioni fra una superficie Hermitiana e una quadrica irriducibile sotto l'ipotesi che esse condividano il piano tangente in un punto. Si caratterizzano inoltre in termini geometrici i casi estremali.

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

Sia $\mathcal{S}$ una $(t-1)$-fibrazione desarguesiana di PG$(rt-1,q)$, $\Pi$ un fissato sottospazio $m$-dimensionale $\Lambda$ il sottoinsieme lineare (*linear set*) identificato dagli elementi di $\mathcal{S}$ con intersezione non vuota con $\Pi$. È ben noto che l'immersione di Plücker degli elementi di $\mathcal{S}$ è una varietà algebrica $\mathcal{V}_{rt}$. In questo lavoro si descrive l'immagine sotto l'immersione di Plücker degli elementi di $\Lambda$ e si dimostra che è una varietà algebrica $m$-dimensionale, proiezione di una varietà di Veronese di dimensione $m$ e grado $t$ e che tale varietà è una sezione lineare di $\mathcal{V}_{rt}$.

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

In questo lavoro si introduce la famiglia dei codici lineari di Grassmann di tipo simplettico, costruita a partire da Grassmanniane polari di tipo simplettico, in modo analogo ai codici di Grassmann ordinari e ai codici di Grassmann ortogonali. I codici lagrangiani-grassmanniani sono uno sottofamiglia di tali codici. In particolare, si determinano tutti i parametri dei codici simplettici associati a Grassmanniane di rette e si fornisce l'enumeratore dei pesi completo per i codici di tipo lagrangiano-grassmanniano di rango 2 e di rango 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).

I codici di Grassmann di tipo ortogonale sono stati introdotti in [I. Cardinali, L. Giuzzi, *Codes and Caps from Orthogonal Grassmannians*]. In questo lavoro si determina in modo esplicito la distanza minima per i codici di questo tipo che nascono da grassmanniane di rette, sotto l'ipotesi che la caratteristica del campo sia dispari.

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

Si determina la lista completa di tutte le possibili intersezioni di una superficie Hermitiana $\mathcal{H}$ con una quadrica irriducibile di PG$(3, q^2)$, sotto l'ipotesi che esse abbiano in comune almeno un piano tangente (ad un punto semplice) nel caso $q$ pari.

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

In questo articolo si costruiscono dei nuovi sottoinsiemi minimali di AG$(r, q^2)$ che posseggono esattamente 3 intersezioni con gli iperpiani. Tali insiemi sono poi utilizzati per costruire dei codici correttori proiettivi con pochi pesi, di cui determiniamo esplicitamente il polinomio enumeratore. Inoltre si costruiscono nuove famiglie di multiinsiemi a 3 caratteri in PG$(r, q^2)$ con $r$ pari e si calcola la distribuzione dei pesi dei codici ad esse associati.

▷ A Geometric Approach to Alternating $k$-linear Forms
I. Cardinali, L. Giuzzi, A. Pasini, J. Algebraic Combin. 45: 931–963 (2017).

Sia $V$ uno spazio vettoriale di dimensione finita $n$ su di un campo arbitrario $\mathbb{K}$. Fissato $2 \leq k \leq n-1$, esiste una corrispondenza biiettiva naturale fra le forme $k$-multilineari alternanti $\varphi$ definite su $V$ e i funzionali lineari $f : \wedge^k V \to \mathbb{K}$. Sia ora $\varepsilon_k : \mathcal{G}_k(V) \to \text{PG}(\wedge^k V)$ l'immersione di Plücker della $k$-Grassmanniana $\mathcal{G}_k(V)$ di $V$. Allora $\varepsilon_k^{-1}(\ker(V) \cap \varepsilon_k(\mathcal{G}_k(V)))$ risulta essere un iperpiano della geometria punto-retta $\mathcal{G}_k(V)$. È ben noto che ogni iperpiano di $\mathcal{G}_k(V)$ può ottenersi in questo modo; in altre parole, ogni iperpiano di $\mathcal{G}_k(V)$ è la famiglia dei $k$-sottospazi di $V$ over una fissata forma $k$-multilineare alternante si annulla identicamente.

Fissato ora un iperpiano $H$ di $\mathcal{G}_k(V)$, sia $R^{\uparrow}(H)$ il sottospazio di $\mathcal{G}_{k-1}(V)$ formato dai $(k-1)$-sottospazi $A \subseteq V$ tali che $H$ contenga tutti i $k$-sottospazi $X$ con $A \subseteq X$. In altre parole, se $\varphi$ è una forma $k$-multilineare alternante che definisce $H$ (tale forma è unica a meno di fattori scalari), allora gli elementi di $R^{\uparrow}(H)$ sono i $(k-1)$-sottospazi $A = (a_1, \ldots, a_{k-1})$ tali che $\varphi(a_1, \ldots, a_{k-1}, x) = 0$ per ogni $x \in V$. In linea di principio, se $n-k$ è pari, allora è possibile che si abbia $R^{\uparrow}(H) = \emptyset$. Quando $n-k$ è dispari, sicuramente $R^{\uparrow}(H) \neq \emptyset$, in quanto ogni $(k-2)$-sottospazio di $V$ è contenuto in almeno un elemento di $R^{\uparrow}(H)$; d'altro canto, in questo caso, può accadere che ogni $(k-2)$-sottospazio di $V$ sia contenuto in *esattamente* un elemento di $R^{\uparrow}(H)$. Se tale situazione si verifica si dice che $R^{\uparrow}(H)$ è di tipo *spread-like*. In questo lavoro si ottengono alcuni risultati su $R^{\uparrow}(H)$ che risolvono delle questioni aperte presenti in letteratura; inoltre si presenta la congettura che se $n-k$ è pari e almeno 4, allora $R^{\uparrow}(H) \neq \emptyset$ con la sola eccezione di $\mathbb{K} \leq \mathbb{R}$ e $(n,k) = (7,3)$, mentre se $n-k$ è dispari e almeno 5, allora $R^{\uparrow}(H)$ non è mai di tipo *spread-like*.

▷ Enumerative coding for Line Polar Grassmannians with applications to codes
I. Cardinali, L. Giuzzi, Finite Fields Appl. 46: 107–138 (2017).

Una $k$-Grassmanniana polare è una geometria che ha come punti l'insieme di tutti i sottospazi $k$-dimensionali di uno spazio vettoriale $V$ che sono totalmente isotropi per una assegnata forma bilineare $\mu$ non degenere definita su $V$. In particolare la si può considerare come una sottogeometria della usuale $k$-Grassmanniana proiettiva. In questo lavoro consideriamo Grassmanniane di rette di tipo ortogonale e simplettico, i.e. supponiamo $k = 2$ e che $\mu$ sia una forma bilineare non degenere di tipo simmetrico o alternante. In particolare, forniamo un metodo per enumerare e costruire efficentemente i loro punti. Questo ha diverse applicazioni pratiche; fra esse discuteremo alcune strategie di codifica/decodifica/correzione di errore per i codici di Grassmann polari di entrambi i tipi.

▷ A geometric approach to alternating $k$-linear forms

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

Dato uno spazio vettoriale $V$ di dimensione $n$ su di un campo $\mathbb{K}$, sia $2 \leq k < n$. Vi è una corrispondenza naturale fra le forme $k$-multilineari alternanti su $V$ e i funzionali lineari su $\bigwedge^k V$. In particolare una forma alternante $\varphi$ ed un funzionale $f$ si corrispondono quando $\varphi(x_1, \ldots, x_k) = f(x_1 \wedge \ldots \wedge x_k)$ per ogni $x1, \ldots, x_k \in V$. Sia ora $\varepsilon_k : \mathcal{G}_k(V) \to \mathrm{PG}(\bigwedge^k V)$ l'immersione di Plücker della $k$-Grassmanniana $\mathcal{G}_k$ di $V$. Allora, $\varepsilon^{-1}(\ker(f) \cap \varepsilon_k(\mathcal{G}_k(V)))$ è un iperpiano $H$ della geometria punto-retta $\mathcal{G}_k(V)$. È ben noto che ogni iperpiano$H$ di $\mathcal{G}_k(V)$ si può ottenere in tale modo. Definiamo ora per ogni iperpiano $H$ l'insieme $R^{\uparrow}(H)$ come il sottoinsieme di $\mathcal{G}_{k-1}(V)$ formato dai $(k-1)$-sottospazi $A \leq V$ tali che $H$ contenga tutti i $k$-sottospazi contenenti $A$. In particolare, quando $n-k$ è pari è possibile, a priori, che $R^{\uparrow}(H)$ sia vuoto, ma per $n-k$ dispari sicuramente $R^{\uparrow}(H) \neq \emptyset$. In effetti, per $n-k$ dispari può accadere che ogni $(k-2)$-spazio di $V$ sia contenuto in esattamente un elemento di $R^{\uparrow}(H)$. In tal caso diremo che $R^{\uparrow}(H)$ è *spread-like*. In questo lavoro ottieniamo alcuni risultati su $R^{\uparrow}(H)$ risolvendo alcune questioni aperte; in particolare si congettura che se $n-k \geq 4$ è pari, allora $R^{\uparrow}(H) \neq \emptyset$ tranne che per il caso $\mathbb{K} \leq \mathbb{R}$ e $(n,k) = (7,3)$, mentre se $n-k \geq 5$ è dispari $R^{\uparrow}(H)$ non è mai *spread-like*.

▷ On transparent embeddings of point-line geometries

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

In questo lavoro si introduce la classe delle immersioni trasparenti di geometrie punto retta $\Gamma = (\mathcal{P}, \mathcal{L})$ come la classe di tutte le immersioni proiettive piene $\varepsilon : \Gamma \to \mathrm{PG}(V)$ tali che la preimmagine di ogni retta proiettiva interamente contenuta in $\varepsilon(\mathcal{P})$ sia una retta di $\Gamma$ (i.e. un elemento di $\mathcal{L}$). In particolare studiamo la trasparenza delle immersioni di Plücker di grassmanniane proiettive e polari e delle immersioni *spin* di geometrie *half–spin* e spazi polari duali di tipo ortogonali. Come applicazioni di questi risultati, si deducono diversi risultati simili al teorema di Chow per le grassmanniane polari e le geometrie *half–spin*.

▷ Minimum distance of Line Orthogonal Grassmann Codes in even characteristic

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

In questo lavoro si determina la distanza minima per codici che nascono da Grassmanniane ortogonali di rette nel caso di caratteristica $q$ pari. Il caso $q$ dispari è già stato risolto in "I. Cardinali, L. Giuzzi, K. Kaipa, A. Pasini, Line Polar Grassmann Codes of Orthogonal Type, J. Pure Applied Algebra." Inoltre si dimostra che per $q$ pari tutte le parole di peso minimo sono equivalenti e che i codici che nascono da Grassmanniane simplettiche di rette sono sottocodici propri di codimensione $2n$ di quelli ortogonali.

▷ Line Hermitian Grassmann Codes and their Parameters

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

In questo lavoro si introducono codici lineari da Grassmanniane Hermitiane di rette e se ne determinano i parametri e le parole di peso minimo.

▷ Identifiers for MRD codes

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

Per ogni valore ammissibile dei parametri $n$ e $k$ esistono $[n,k]$-MRD codici $\mathbb{F}_q$-lineari. In effetti, si può dimostrare che se si considerano estensioni di campo abbastanza grandi, allora quasi tutti i codici con la metrica del rango sono MRD. D'altro canto, poche famiglie di codici con tali proprietà sono correntemente note. In questo lavoro si studiano alcuni invarianti di codici MRD che vengono valutati sulle famiglie note, fornendo in tal modo una nuova caratterizzazione dei codici di Gabidulin.

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

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

Sia $\mathcal{G}_k(V)$ la $k$–Grassmanniana di uno spazio vettoriale $V$ con $\dim V = n$. Assegnato un iperpiano $H$ di $\mathcal{G}_k(V)$, 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] si è definita una sottogeometria punto–retta di $\mathrm{PG}(V)$ chiamata *geometria dei poli di* $H$. In questo lavoro, sfruttando la classificazione delle forme trilineari alternanti in dimensione bassa, caratterizziamo le possibili geometrie dei poli per $k = 3$ e $n \leq 7$ e proponiamo alcune nuove costruzioni. Estendiamo inoltre un risultato di J. Draisma e R. Shaw relativo l'esistenza di fibrazioni di $\mathrm{PG}(5, \mathbb{K})$ che nascono da iperpiani di $\mathcal{G}_3(V)$.

▷ Grassmann embeddings of polar Grassmannians

I. Cardinali, L. Giuzzi, A. Pasini, preprint

In questo lavoro si calcola la dimensione dell'immersione di Grassmann delle Grassmanniane polari associate con forme eventualmente degeneri di tipo Hermitiano, alternante o quadratico con indice di Witt non necessariamente massimale. Inoltre in caratteristica 2 si definisce per forme quadratiche non degeneri una generalizzazione della cosiddetta immersione di Weyl e si dimostra che l'immersione di Grassmann è un quoziente di questa.

▷ Implementing Line-Hermitian Grassmann codes

I. Cardinali, L. Giuzzi, preprint

In [I. Cardinali and L. Giuzzi. Line Hermitian Grassmann codes and their parameters. Finite Fields Appl., 51: 407-432, 2018] si sono introdotti dei codici associati a Grassmanniane polari di rette di tipo ortogonale. In questo lavoro, seguendo l'approccio di [I. Cardinali and L. Giuzzi. Enumerative coding for line polar Grassmannians with applications to codes. Finite Fields Appl., 46:107-138, 2017], forniamo un algoritmo per l'enumeratore dei punti di una Grassmanniana Hermitiana di rette.