

GRUPPO DI RICERCA

Galois geometries and their applications (Geometrie di Galois e loro applicazioni)

1. DATI IDENTIFICATIVI DEL GRUPPO DI RICERCA

Categorie ERC	<ul style="list-style-type: none"> - PE1_16 - Discrete mathematics and combinatorics - PE1_17-Mathematical aspects of computer science - PE1_2-Algebra
Settore Scientifico Disciplinare	<p>MATH-02/B (Geometry)</p> <p>MATH-02/A (Algebra)</p>
Parole Chiave (Keywords)	<ul style="list-style-type: none"> - Galois geometry - Finite field - Incidence structure - Finite geometry - Linear code - Polynomials over finite fields - Linear and nonlinear functions over finite fields

2. COMPOSIZIONE E COORDINAMENTO

Responsabile Scientifico / Coordinatore:

- **Nome e Cognome:** [Olga Polverino]
- **Qualifica:** [Professore Ordinario]
- **Email:** [olga.polverino@unicampania.it]
- **Link Orcid Personale** 0000-0002-5588-3352

Componenti del Gruppo:

- 1) **Vito Napolitano**, docente 2^a fascia presso il DMF; numero ID ORCID 0000-0002-2504-6967
- 2) **Ferdinando Zullo**, ricercatore di tipo B presso il DMF; numero ID ORCID 0000-0002-5087-2363
- 3) **Usman Mushrraf**, dottorando del DMF XXXIX ciclo; ID ORCID 0009-0006-0259-4377
- 4) **Paolo Santonastaso**, contrattista di ricerca presso il Politecnico di Bari; numero ID ORCID 0000-0002-9525-7049
- 5) **Maria Montanucci**, professore ordinario presso la Technical University of Denmark, Danimarca; numero ID ORC 0000-0002-1226-3209
- 6) **Geertrui Van de Voorde**, professore associato presso la School of Mathematics and Statistics dell' University of Canterbury, New Zealand, numero ID ORCID 0000-0002-4957-6911
- 7) **Martino Borello**, professore associato presso l'Université Paris 8, France, numero ID ORCID 0000-0002-4597-1244

3. ATTIVITÀ SCIENTIFICA E NETWORK

Breve Descrizione delle linee di ricerca:

L'attività del gruppo è dedicata allo studio delle Geometrie su campi di Galois nei loro aspetti combinatori, geometrici, algebrici, computazionali e algoritmici, con particolare attenzione alle applicazioni e alle connessioni con teoria dei disegni, codici, grafi e crittografia. Le principali linee di ricerca sono tra loro strettamente integrate.

L1) Insiemi lineari. *Costituiscono sottostrutture di spazi proiettivi su campi finiti che generalizzano le sottogeometrie classiche. Sono impiegati nella classificazione di oggetti geometrici e algebrici e nella costruzione di nuove famiglie di esempi, con applicazioni a semicorpi, blocking sets e codici lineari nelle metriche di Hamming, rango e sum-rank. L'obiettivo è costruire e classificare insiemi con proprietà legate ai parametri ottimali dei codici.*

L2) Strutture di incidenza. *La ricerca mira a ricostruire strutture finite a partire da relazioni aritmetiche o proprietà geometriche, studiando insiemi di punti tramite le loro intersezioni con sottospazi. Tali strutture forniscono una descrizione geometrica dei codici lineari e permettono risultati di classificazione e nuove costruzioni ispirate a varietà algebriche classiche.*

L3) Polinomi su campi finiti. *L'attenzione è rivolta ai polinomi linearizzati, ai polinomi di permutazione e alle funzioni Almost Perfect Nonlinear, rilevanti per le applicazioni crittografiche.*

L4) Codici lineari e crittografia. Il gruppo sviluppa metodi algebrici e geometrici per progettare codici efficienti e studiarne codifica e decodifica, con applicazioni anche alla crittografia post-quantistica basata su codici.

Collaborazioni Nazionali ed Internazionali:

(Indicare Università, Enti di ricerca o Aziende con cui si hanno progetti o pubblicazioni in comune)

- **Nazionali:** [Università di Napoli Federico II, Università di Padova, Università di Perugia, Università di Modena e Reggio Emilia, Politecnico di Bari]
- **Internazionali:** [Technical University of Denmark , University of Canterbury, INRIA Saclay, Université Paris 8, Technical University of Munich, Virginia Tech]

4. PROGETTI, BREVETTI E PUBBLICAZIONI

Principali Progetti di Ricerca e Brevetti:

a) Progetti Internazionali

1. Titolo Progetto “The combinatorics of minimal codes and security aspects”, 2023-2024, , financed by French Embassy in Italy and Laboratory Ypatia of Mathematical Sciences, Cnrs/INdAM - Cassini call., componenti DMF: C. Castello, V. Napolitano, O. Polverino, P. Santonastaso, F. Zullo (PI); componenti unità francese: M. Borello, M. Scotti.
2. Titolo Progetto “Algebraic and Geometric methods in coding theory”, 2024-2025, financed by Bando Galilei 2024. Componenti DMF C. Castello, O. Polverino, P. Santonastaso, F. Zullo (PI),
3. Titolo del progetto "New geometric perspectives for error-correcting codes", 2026-2028, financed by Marsden Fund Award 2025, New Zealand. cCVomponent DMF co-PI F. Zullo (PI G. Van de Voorde, University of Canterbury),

b) Progetti nazionali (PRIN, bandi PNRR, etc.) o di ateneo.

4. Titolo Progetto “PQCrypto”, componenti DMF: O. Polverino, G. Zini (PI), F. Zullo, 2020-2021, finanziato da Unicampania, (Bando di Ateneo per il finanziamento di progetti di ricerca fondamentale ed applicata dedicato ai giovani Ricercatori, VALERE).
5. Titolo Progetto “COMBINE”, 2023-2024 componenti DMF C. Castello, S. Khan, V. Napolitano, O. Polverino, M. Raimondo, P. Santonastaso, F. Zullo (PI), finanziato da Unicampania, (Bando

di Ateneo per il finanziamento di progetti di ricerca fondamentale ed applicata dedicato ai giovani Ricercatori).

6. Titolo Progetto: “Functional Encryption for cloud encryption” 2023-2025, componenti DMF M. Ferrara (assegnista), P. Santonastaso (assegnista), co-PI F. Zullo (altro co-PI A. Tortora) finanziato da Fondazione Bruno Kessler <https://www.fbk.eu/it/>.
7. Titolo Progetto: “A mathematical approach to inverse problems arising in cultural heritage preservation and dissemination”, 2023-2025, co-PI e responsabile di unità Unicampania F. Zullo finanziato dal MUR, bando PRIN-PNRR 2022.
8. Titolo Progetto: “Geometric and computational methods in coding theory”, 2023-2025, PI V. Napolitano, O. Polverino, P. Santonastaso, C. Castello, F. Moretta and F. Zullo, (Bando di ateneo: Avviso pubblico di selezione per il finanziamento di progetti D.R. 111 del 09/02/2024)

Principali Pubblicazioni Recenti:

(Elencare le pubblicazioni più rappresentative prodotte dal gruppo negli ultimi 5 anni)

1. [C. Castello, H. Gluesing-Luerssen, O. Polverino, F. Zullo], *Quasi-optimal cyclic orbit codes*, **Designs, Codes, and Cryptography**, 2026. DOI: 10.1007/s10623-025-01751-4.
2. [U. Mushraf, F. Zullo], *One weight codes in the sum-rank metric*, **Finite Fields and their Applications**, 2026, DOI: [10.1007/s00013-025-02145-7]
3. [Y. Zhong, S. Hayat, S. Khan, V. Napolitano, A. Mohammed], *Combinatorial analysis of line graphs: domination, chromaticity, and Hamiltonianity*, **AIMS Mathematics**, 2025, DOI: 10.3934/math.2025599.
4. [V. Smaldore, C. Zanella, F. Zullo] *On the stabilizer of the graph of linear functions over finite fields*, **Forum Mathematicum**, 2025, DOI: 10.1515/forum-2023-0353.
5. [C. Castello, O. Polverino, F. Zullo], *Full weight spectrum one-orbit cyclic subspace codes*, **Journal of Combinatorial Theory. Series A**, 2025. DOI: [10.1016/j.jcta.2024.106005]
6. [G. Cotardo, G. Ravagnani, F. Zullo], *Whitney numbers of rank-metric lattices and code enumeration*, **Advances in Applied Mathematics**, 2025, DOI: 10.1016/j.aam.2025.102938.
7. [P. Santonastaso, F. Zullo] *Invariants for sum-rank metric codes*, **Annali di Matematica Pura ed Applicata**, 2025, DOI: 10.1007/s10231-025-01640-6.

8. [O. Polverino, P. Santonastaso, F. Zullo], *MAXIMUM WEIGHT CODEWORDS OF A LINEAR RANK-METRIC CODE*, **SIAM Journal on Discrete Mathematics**, 2024. DOI: 10.1137/23M1584812.
 9. [V. Napolitano, O. Polverino, P. Santonastaso, F. Zullo], *Clubs and Their Applications*, **SIAM Journal on Applied Algebra and Geometry**, 2024, DOI: 10.1137/22M1523534.
 10. [M. Borello, F. Zullo], *Geometric dual and sum-rank minimal codes*, **Journal of Combinatorial Designs**, 2024, DOI: 10.1002/jcd.21934.
 11. [G. Alfarano, A. Neri, F. Zullo]: *Maximum flag-rank distance codes*, **Journal of Combinatorial Theory. Series A**, 2024, DOI: 10.1016/j.jcta.2024.1059008
 12. [C. Castello, O. Polverino, P. Santonastaso, F. Zullo], *Constructions and equivalence of Sidon spaces*, **Journal of Algebraic Combinatorics**, 2023. DOI: [10.1007/s10801-023-01275-x]
 13. [A. Gruica, A. Ravagnani, J. Sheekey, F. Zullo], *Rank-metric codes, semifields, and the average critical problem*, **SIAM Journal on Discrete Mathematics**, (2023), DOI: [10.1137/22M1486893]
 14. [O. Polverino, P. Santonastaso, J. Sheekey, F. Zullo], *Divisible linear rank metric codes*, **IEEE Transactions on Information Theory**, 2023. DOI: [10.1109/TIT.2023.3241780]
 15. [V. Napolitano, O. Polverino, P. Santonastaso, F. Zullo], *Linear sets on the projective line with complementary weights*, **Finite Fields and their Applications**, 2022. DOI: [10.1016/j.ffa.2020.101798]
 16. [D. Bartoli, M. Calderini, O. Polverino, F. Zullo,], *On the infiniteness of a family of APN functions*, **Journal of Algebra**, 2022. DOI: [10.1016/j.jalgebra.2022.01.026]
 17. [V. Napolitano, O. Polverino, P. Santonastaso, F. Zullo], *Linear sets on the projective line with complementary weights*, **Discrete Mathematics**, 2022. DOI: [10.1016/j.disc.2022.112890]
 18. [B. Csajb\`ok, G. Marino, O. Polverino, F. Zullo], *Generalising the Scattered Property of Subspaces*, **Combinatorica**, 2021. DOI: [10.1007/s00493-020-4347-y]
 19. [O. Polverino, G. Zini, F. Zullo], *On certain linearized polynomials with high degree and kernel of small dimension*, **Journal of Pure and Applied Algebra**, 2021, DOI: [10.1016/j.jpaa.2020.106491]
 20. [V. Napolitano, O. Polverino, G. Zini, F. Zullo], *Linear sets from projection of Desarguesian spreads*, **Finite Fields and their Applications**, 2021, DOI:[10.1016/j.ffa.2020.101798]
-