

GIANIRA NICOLETTA ALFARANO

gianiranicoletta.alfarano@math.uzh.ch

University of Zurich, Department of Mathematics

Winterthurerstrasse 190, 8057 Zurich, Switzerland

PERSONAL INFORMATION

Birthplace Noci (Bari), Italy

Birthdate 01/11/1993

Citizenship Italian

ORCID <https://orcid.org/0000-0002-7463-6365>

ArXiv ID <https://arxiv.org/a/0000-0002-7463-6365>

Researchgate https://www.researchgate.net/profile/Gianira_Alfarano

RESEARCH INTERESTS

Algebraic coding theory, combinatorics, finite geometry, applied discrete mathematics, commutative algebra, cryptography.

EDUCATION

University of Zurich, Switzerland

April 2018–current

Department of Mathematics

Ph.D. student in Applied Algebra

Advisor: Prof. Dr. Joachim Rosenthal

Università degli Studi di Trento, Italy

2015–2017

Master of Mathematics - Curriculum Coding Theory and Cryptography

Master degree in Mathematics *Grade: 110/110 cum Laude*

Master thesis title: The Diffusion Property of some Mixing-Layers

Università del Salento, Lecce, Italy

2012–2015

Bachelor of Mathematics

Bachelor degree in Mathematics *Grade: 110/110 cum Laude*

Bachelor thesis title: The classical unital

Liceo Scientifico “Leonardo da Vinci”, Noci, Italy

2007–2012

High school

High school diploma *Grade: 100/100 cum Laude*

POSITIONS HELD

Teaching Assistant/Ph.D. student

April 2018–current

University of Zurich

Advisor: Prof. Dr. Joachim Rosenthal

Research Stage

February–June 2017

Topic: Symmetric Cryptography

HORST GÖRTZ INSTITUTE FOR IT-SECURITY (HGI),

Ruhr Universität

Bochum, Germany

AWARDS AND GRANTS

- UZH Alumni grant** 2022
Additional grant for the organization of the Summer School
“ACT 22: Algebraic Coding Theory”
- Ph.D Mobility Fellowship** February–August 2021
Financial support from the Swiss National Science Foundation
for 6-months scientific visit
University College Dublin, Ireland.
- Grant GRC 2019_Q3_G_003** 2020
Grant for the organization of the Summer School
“ACT 22: Algebraic Coding Theory”
- VAUZ** 2020
Additional grant for the organization of the Summer School
“ACT 21: Algebraic Coding Theory”
- Financed through the Swiss National Science Foundation grant no. 188430** 2019 – 2022
P.I. Prof. J. Rosenthal
- Oberwolfach Leibniz Graduate Student (OWLG)** March 2019
grant to participate to the
Oberwolfach Workshop 1912, Contemporary Coding Theory
Oberwolfach, Germany.
- Schloss Dagstuhl - Leibniz Center for Informatics** December 2018
Invitation to participate to the seminar
“Algebraic Coding Theory for Networks, Storage, and Security” (18511), Germany.

OTHER AWARDS

- Travel Grant** 30 May- 3 June 2022
Partial financial support for “Combinatorics 2022” from the local committee, in Mantua, Italy.

ACADEMIC VISITS

- Invited researcher at University of Paris VIII, France, 5-18 September 2021.
- Invited researcher at the Max Planck Institute for Mathematics in the Sciences (MiS) in Leipzig, Germany, July-August 2021.
- Researcher at University College Dublin, Ireland, February–August 2021
- Invited researcher at the Max Planck Institute for Mathematics in the Sciences (MiS) in Leipzig, Germany, 21-23 September 2020.
- Invited researcher at the Universidad de Alicante, Alicante, Spain, May-June 2019.
- Research stage at HORST GÖRTZ INSTITUTE FOR IT-SECURITY (HGI), Ruhr Universität, Bochum, Germany, February-June 2017

PUBLICATIONS IN PEER-REVIEWED JOURNALS

10. **G. N. Alfarano**, M. Borello, A. Neri, and A. Ravagnani. Linear Cutting Blocking Sets and Minimal Codes in the Rank Metric. *Accepted for publication in Journal of Combinatorial Theory, Series A*, **2022**.
arXiv version, <https://arxiv.org/abs/2106.12465>
9. **G. N. Alfarano**, A. Gruica, J. Lieb, J. Rosenthal. Convolutional codes over finite chain rings, MDP codes and their characterization. *Advances in Mathematics of Communications*, **2022**
arXiv version, <https://arxiv.org/abs/2104.09486>
8. **G. N. Alfarano**, F.J. Lobillo, A. Neri, A. Wachter-Zeh. Sum-rank product codes and bounds on the minimum distance. *Finite Fields and their Applications*, **2022**.

DOI: 10.1016/j.ffa.2022.102013
7. **G. N. Alfarano**, M. Borello, A. Neri, and A. Ravagnani. Three Combinatorial Perspectives on Minimal Codes. *Siam Journal on Discrete Mathematics*, **2021**.

DOI: 10.1137/21M1391493
6. **G. N. Alfarano**, J. Lieb, J. Rosenthal. Construction of LDPC convolutional codes via difference triangle sets. *Designs, Codes and Cryptography*, **2021**

DOI: 10.1007/s10623-021-00912-5
5. **G. N. Alfarano**, K. Khathuria, V. Weger. A survey on single server private information retrieval in a coding theory perspective. *Applicable algebra in engineering communication and computing*, **2021**

DOI: 10.1007/s00200-021-00508-5
4. **G. N. Alfarano**, F.J. Lobillo, and A. Neri. Roos bound for skew cyclic codes in Hamming and rank metric. *Finite Fields and Their Applications*, 69: 101772, **2021**.

DOI: 10.1016/j.ffa.2020.101772
3. **G. N. Alfarano** and J. Lieb. On the left primeness of some polynomial matrices with applications to convolutional codes. *Journal of Algebra and its applications*, **2020**.

DOI: 10.1142/S0219498821502078
2. **G. N. Alfarano**, M. Borello, and A. Neri. A geometric characterization of minimal codes and their asymptotic performance. *Advances in Mathematics of Communications*, **2020**.

DOI: 10.3934/amc.2020104
1. **G. N. Alfarano**, C. Beierle, T. Isobe, S. Kölbl, G. Leander. ShiftRows Alternatives for AES-like Ciphers and Optimal Cell Permutations for Midori and Skinny. *IACR Transactions of Symmetric Cryptology*. 2018(2): 20-47, **2018**.

DOI: 10.13154/tosc.v2018.i2.20-47

REFEREED CONFERENCE PROCEEDINGS

2. **G. N. Alfarano**, A. Ravagnani, E. Soljanin. Dual-Code Bounds on Multiple Concurrent (Local) Data Recovery. *2022 IEEE International Symposium on Information Theory (ISIT)*, **2022**.
arXiv version, <https://arxiv.org/abs/2201.07503>

1. **G. N. Alfarano**, J. Lieb, and J. Rosenthal. Construction of Rate $(n - 1)/n$ Non-Binary LDPC Convolutional Codes via Difference Triangle Sets. *2020 IEEE International Symposium on Information Theory (ISIT)*, pp. 138-143, **2020**.

DOI: 10.1109/ISIT44484.2020.9174510.

PREPRINTS

3. **G. N. Alfarano**, E. Byrne, The Cyclic Flats of a q -Matroid. *submitted*, **2022**.
arXiv version, <https://arxiv.org/abs/2204.02353>
2. **G. N. Alfarano**, K. Khathuria, and S. Tinani. On Cyclic Matroids and their Applications. *submitted*, **2021**.
arXiv version, <https://arxiv.org/abs/2107.14214>
1. **G. N. Alfarano**, D. Napp, A. Neri, and V. Requena. Weighted Reed-Solomon convolutional codes. *submitted*, **2020**.
arXiv version, arxiv.org/abs/2012.11417

INVITED TALKS

10. Max Planck Institute for Mathematics in the Sciences, Leipzig, Germany, “ q -Analogues of matroids and codes”, April 2022.
9. Sabanci Algebra Seminar, University of Sabanci, Turkey, “(Linear) cutting blocking sets and minimality of codes”, October 2021
8. PICS, Postgraduate International Coding theory Seminar, “(Linear) cutting blocking sets and their codes”, September 2021.
7. Seminar Discrete Mathematics, Codes and Cryptography - University of Paris 8, “Bounds on the distance of skew cyclic codes”, September 2021.
6. De Cifris, Schola Latina Seminars, “A geometric interpretation of minimal code”, May 2021.
5. Maths Postgraduate Seminar Series, University College Dublin, “Geometric aspects of minimal linear codes”, March 2021.
4. eSeminar UGent-VUB, “The geometry of minimal linear codes”, March 2021.
3. Zurich Graduate Colloquium, Zurich, Switzerland, “What is...a convolutional code?”, December 2019.
2. University of Alicante, Alicante, Spain, “ σ -Quasicyclic and Projective Convolutional Codes”, June 2019.
1. Research Seminars, University of Trento, Trento, Italy, “An introduction to Convolutional Codes”, June 2018.

OTHER TALKS

3. First Annual Conference: Cryptography and Coding Theory, “Roos-like bound for skew-cyclic codes in Hamming and (sum-)rank metric”, September 2021.
2. IEEE International Symposium on Information Theory (ISIT), “Construction of Rate $(n - 1)/n$ Non-Binary LDPC Convolutional Codes via Difference Triangle Sets, Los Angeles, California, (virtual conference) June 2020.

1. Arbeitsgemeinschaft in Codierungstheorie und Kryptographie, University of Neuchatel, Switzerland, New “Algebraic Construction of MDP Convolutional Codes”, December 2019.

OTHER ACTIVITIES

“Matematica per la crittografia” May-June 2021
Laboratory of Cryptography for High School Students, 6 hours, in italian.
Liceo Scientifico, Leonardo da Vinci, Noci, Italy.

WORKSHOPS AND CONFERENCES ATTENDED

Summer School: “ACT 20: Algebraic Coding Theory (ACT)” June 2021
virtual summer school
Zurich, Switzerland

International Workshop on the Arithmetic of Finite Fields (WAIFI) 2020 July 2020
virtual conference
Rennes, France.

IEEE International Symposium on Information Theory (ISIT) 2020 June 2020
virtual conference
Los Angeles, California, USA

Munich Workshop on Coding and Cryptography 2019 July 2019
Technische Universität München, Germany

SIAM Conference on Applied Algebraic Geometry July 2019
Bern, Switzerland

Summer School: “Finite Geometry & Friends” June 2019
Vrije Universiteit Brussel, Belgium

Oberwolfach Workshop 1912 March 2019
Contemporary Coding Theory
Germany

Dagstuhl Seminar 18511 December 2018
Algebraic Coding Theory for Networks, Storage, and Security
Germany

CIMPA Research School and Workshop August–September 2018
Quasi-Cyclic and Related Algebraic Codes
Ankara, Turkey

Summer School: Number theory and coding theory, contemporary applications in security May–June 2018
Turku, Finland

Munich Workshop on Coding and Cryptography 2018 April 2018
Technische Universität München, Germany

TEACHING EXPERIENCE

Lecturer and Organizer

February 2022–June 2022

MAT011 Matroids theory
University of Zurich, Switzerland

Teaching Assistant

April 2018–current

University of Zurich, Switzerland
 Duties: frontal lectures, exercise classes,
 preparation and correction of exams and homeworks.

MAT476 Finite Fields, Theory and Applications (Fall 2020)

MAT512 Elliptic curves (Spring 2018, Spring 2020)

MAT001 Kryptographie (Fall 2019)

MAT005 Codierungstheorie (Spring 2019)

MAT211 Algebra (Fall 2018)

Tutor and Teaching Assistant

March 2015–December 2017

University of Trento, Italy
 Duties: frontal lectures, exercise classes.

Analisi Matematica I

MENTORING EXPERIENCE

Master student co-supervised: S. La Rosa

October 2021 - current

University of Zurich, Switzerland
 jointly with Prof. Dr. J. Rosenthal
 Thesis title: “Minimal Codes and Secret Sharing Schemes”

Master student co-supervised: N. Zürcher

September 2019 - August 2020

University of Zurich, Switzerland
 jointly with J. Rosenthal
 Thesis title: “On the Intractability of Maximum-Likelihood Decoding
 for Reed–Solomon Self-Dual Codes”

Master student co-supervised: A. Gruica

August 2019 - April 2020

University of Zurich, Switzerland
 jointly with J. Rosenthal
 Thesis title: “MDP Convolutional Codes over $\mathbb{Z}/p^r\mathbb{Z}$ ”

ORGANIZATIONAL AND PROFESSIONAL EXPERIENCE

Co-organizer of the Session “Algebraic and Geometric Methods in Coding Theory” for the conference
 “ACA 2022 - Applications of Computer Algebra” August 15 – 19, 2022

Istanbul-Gebze, Turkey
 Link: <https://sites.google.com/view/michela-ceria-home-page/aca-2022-q-mat>

Co-organizer of the events “Female in math get-togethers”

October 2021–current

University of Zurich and ETH Zurich

Co-organizer of the seminars “Zurich Graduate Colloquium”

February 2021–current

Zurich Graduate School in Mathematics

Organizer of “ACT 21: Algebraic Coding Theory e-Summer School”

June 7 – 11, 2021

University of Zurich, Switzerland
Link: <https://www.math.uzh.ch/act/>

Organizer of “ACT 22: Algebraic Coding Theory Summer School”
University of Zurich, Switzerland
Link: <https://www.math.uzh.ch/act/>

July 4 – 8, 2022

Organizer of “Coding Theory and Cryptography,
A conference in honor of
Joachim Rosenthal’s 60th birthday”
University of Zurich, Switzerland
Link: <https://www.math.uzh.ch/aa/index.php?id=32>

July 11 – 15 , 2022

Reviewer for the following scientific journals

2019 - current

“Designs, Codes and Cryptography”

“IEEE, Transactions on Information Theory”

“Advances in Mathematics of Communications”

“Cryptography and Communications”

LANGUAGES

Italian (Mothertongue)

English (Fluent)

French (Basic)