ALLEGATO B

UNIVERSITÀ DEGLI STUDI DI MILANO
selezione pubblica per n._1_ posto/i di Ricercatore a tempo determinato ai sensi dell'art.24,
comma 3, lettera a) della Legge 240/2010 per il settore concorsuale 01/B1 - Informatica___ ,
settore scientifico-disciplinare _____INF/01 - INFORMATICA_____
presso il Dipartimento di __INFORMATICA "GIOVANNI DEGLI ANTONI"_____,
(avviso bando pubblicato sulla G.U. n. ___G.U. 22 _____ del ___17/03/2020___) Codice concorso 4274_

[Michela Ceria]
CURRICULUM VITAE

INFORMAZIONI PERSONALI (NON INSERIRE INDIRIZZO PRIVATO E TELEFONO FISSO O CELLULARE)

COGNOME	**CERIA**
NOME	**MICHELA**
DATA DI NASCITA	[03, 07, 1984]

INSERIRE IL PROPRIO CURRICULUM
(non eccedente le 30 pagine)

Michela Ceria

Academic positions

1 May 2018 - · **University of Milan, Italy** ·
Department of Computer Science · *Postdoc position*: Advanced methods and technologies in Computer Science.

26 April 2017 - 25 April 2018. · **University of Trento, Italy** ·
Department of Mathematics · *Postdoc position*: Algebraic Cryptography and Theory of Cyclic Codes.

07 April 2015 - 06 April 2017 · **University of Trento, Italy** ·
Department of Engineering and Computer Science · *Postdoc position*: Algebraic Cryptography for Online Courses

Awards, Scholarships and grants

French *qualification* to the function of *Maître de Conférences*
Mathematics (11/02/2015 - 31/12/2019, number 15225277843; 31/01/2019 - 31/12/2023, number 19225277843)*Applied Mathematics* (04/02/2015 - 31/12/2019, number 15226277843).

2011-2013 · **PhD scholarship**
Three-year PhD Scholarship, funded by INdAM (National Institution of High Mathematics). INdAM Tutor for the scholarship: Prof. A.*Verra* (University Roma Tre).

Mobility fundings
I got fundings by INdAM (National Institute of high mathematics) to participate to the conferences Current trends on Groebner bases, ICMS2018, PCA2019, ACA2019

May-November 2012 · **Regional fundings**
Regional fundings for the visiting period in Kaiserslautern (Germany).

Research Interests

Combinatorial aspects of Computational Algebra

Commutative and noncommutative Groebner bases

Coding Theory and Cryptography

Computational Algebraic Geometry and Commutative Algebra

For more information see the enclosed Research Statement.

Publications

2020
Why you cannot even hope to use Gröbner bases in cryptography: an eternal golden braid of failures, accepted by the Special issue of Applicable Algebra in Engineering, Communication and Computing, concerning "Computer Algebra and application to combinatorics, coding theory and cryptography". Authors: B. Barkee, M. Ceria, T. Moriarty, A. Visconti.

2020
HELP: a sparse error locator polynomial for BCH codes, accepted by the Special issue of Applicable Algebra in Engineering, Communication and Computing, concerning "Computer Algebra and application to combinatorics, coding theory and cryptography". Authors: M. Ceria, T. Mora, M. Sala .

2019
Zech Tableaux as tools for sparse decoding. accepted for publications in Rendiconti del Seminario Matematico. Authors: M. Ceria, T. Mora, M. Sala.

2019
Bar Code vs Janet tree. Atti della Accademia Peloritana dei Pericolanti, Classe di Scienze Fisiche, Matematiche e Naturali VOL 97, NO 2 (2019) DOI:http://dx.doi.org/10.1478/AAPP.972A6 Author: M. Ceria.

2019
Bar code: a visual representation for finite sets of terms and its applications Math.Comput.Sci. (2019) doi:10.1007/s11786-019-00425-4 Author: M.Ceria

2019
Measuring Performances of a White-box Approach in the IoT Context. Symmetry 2019, 11(8), 1000; https://doi.org/10.3390/sym11081000 Authors: D. Albricci, M. Ceria, A. Shakiba, A. Visconti, F. Cioschi, N. Fornari

2019
Applications of Bar Code to involutive divisions and a greedy algorithm for complete sets. (extended abstract) International Conference Polynomial Computer Algebra '2019 St. Petersburg, Russia April 15-20, 2019 International Euler Institute - ISBN 978-5-96511-1234-0 Author: M. Ceria

2019
Weak involutive bases over effective rings (extended abstract) International Conference Polynomial Computer Algebra '2019 St. Petersburg, Russia April 15-20, 2019 International Euler Institute - ISBN 978-5-96511-1234-0 Author: M. Ceria, T. Mora

2019
A general framework for Noetherian well ordered polynomial reductions Journal of Symbolic Computation,Vol. 95, P. 100-133 ISSN: 0747-7171, https://doi.org/10.1016/j.jsc.2019.02.002 Authors: M. Ceria, T. Mora, M. Roggero

2019
Bar code for monomial ideals. Journal of Symbolic Computation, DOI:https://doi.org/10.1016/j.jsc.2018.06.012 vol. 91, p. 30-56, ISSN: 0747-7171, Author: M. Ceria

2018
Combinatorics of ideals of points: a Cerlienco-Mureddu-like approach for an iterative lex game (abstract) DOI: http://dx.doi.org/10.15304/978841695487 In 24th Conference on Applications of Computer Algebra - ACA 2018: Proceedings, Applications of Computer Algebra, Santiago de Compostela, Spain, June 18-22, 2018. Authors: M. Ceria, T. Mora

2018
Combinatorics of ideals of points: a Cerlienco-Mureddu-like approach for an iterative lex game (extended abstract) International Conference Polynomial Computer Algebra '2018 St. Petersburg, Russia April 16-21, 2018 International Euler Institute - ISBN 978-5-9651-1141-1 Authors: M. Ceria, T. Mora

2018
Efficient computation of squarefree separator polynomials (extended abstract) DOI:https://doi.org/10.1007/978-3-319-96418-8_12 In: Davenport J., Kauers M., Labahn G., Urban J. (eds) Mathematical Software – ICMS 2018. Lecture Notes in Computer Science, vol 10931p. 98-104, Springer, ISBN: 9783319964171, ISSN: 1611-3349, South Bend, 2018, Authors: M. Ceria, T. Mora, A. Visconti.

2017
Buchberger-Zacharias Theory of Multivariate Ore Extensions. DOI: https://doi.org/10.1016/j.jpaa.2017.02.011 *Journal of Pure and Applied Algebra*, vol. 221, p. 2974-3026, ISSN: 0022-4049. Authors: M. Ceria, T. Mora

2017
Bitcoin, la moneta virtuale per transazioni reali, Interlex, may 2017. Authors: M. Ceria, M.Sala

2017
Buchberger-Weispfenning Theory for Effective Associative Rings. DOI:https://doi.org/10.1016/j.jsc.2016.11.008 *Journal of Symbolic Computation*, vol. 83, p. 112-146, ISSN: 0747-7171. Authors: M. Ceria, T.Mora

2016
Bitcoin e Blockchain, Authors: M. Ceria, F. Pintore, M. Sala Aused Informa, 98.

2016
A computational approach to the theory of adjoints. DOI: http://dx.doi.org/10.1478/AAPP.942A7 *Atti della Accademia Peloritana dei Pericolanti, Classe di Scienze Fisiche, Matematiche e Naturali*, vol. 94, p. 1-14, ISSN: 1825-1242. Author: M. Ceria

2015
Term-ordering free involutive bases DOI:10.1016/j.jsc.2014.09.005, *Journal of Symbolic Computation*, vol. 68, p. 87-108, ISSN: 0747-7171, Authors: M. Ceria, T. Mora, M. Roggero

2014
A proof of the "Axis of Evil theorem" for distinct points. Rendiconti del Seminario Matematico, vol. 72, p. 213-233, ISSN: 0373-1243 (2014) Author: M. Ceria

Other accepted works

2019
Bar Code and Janet-like division (extended abstract), accepted for a talk at ACA2019 Authors: M. Ceria.

2019
Weak Involutive bases over effective rings (extended abstract), accepted for a talk at ACA2019 Authors: M. Ceria, T. Mora.

2019
HELP: the knight gambit for efficient decoding of BCH codes (extended abstract), accepted for a talk at ACA2019 Authors: M. Ceria, T. Mora, M. Sala.

2019
Why you cannot even hope to use Gröbner bases in cryptography: an eternal golden braid of failures (extended abstract), accepted for a talk at ACA2019. Authors: B. Barkee, M. Ceria, T. Moriarty, A. Visconti.

2019
Combinatorial decompositions for monomial ideals (extended abstract), accepted for the poster presentation at MEGA2019. Authors: M. Ceria.

2018
Combinatorics of ideals of points: a Cerlienco-Mureddu-like approach for an iterative lex game Accepted for a talk at *ACA 2018*, *PCA 2018* Authors: M. Ceria, T. Mora.

2017
On the discrete logarithm problem for prime-field elliptic curves Accepted for a computation presentation at *MEGA 2017*. Authors: A. Amadori, M. Ceria, F. Pintore, M. Sala

Submitted works

2020
Constructions of new matroids and designs over $GF(q)$, Authors: E. Byrne, M. Ceria, S. Ionica, R. Jurrius, E. Saçikara

2020
Why you should not even think to use Ore algebras in Cryptography., Author: M. Ceria, T. Mora, A. Visconti.

2020
Applications of Bar Code to involutive divisions and a greedy algorithm for complete sets., Author: M. Ceria

2019
Toward involutive bases over effective rings, Authors: M. Ceria, T. Mora

2019
A trojan Diffie-Hellman-like protocol based on proof of gullibility, Authors: M. Ceria, A. De Piccoli, T. Moriarty and A. Visconti.

2019
Sublime Experience: new strategies for measuring the aesthetic impact of the sublime Authors: M. Mazzocut-Mis, A. Visconti, H. Tahayori and M. Ceria

2019
Combinatorial decompositions for monomial ideals , Author: M. Ceria

Available in Arxiv

2019
Macaulay, Lazard and the Syndrome Variety arXiv:1910.13189 [math.CO]. Authors: M. Ceria.

2017
Combinatorics of involutive Divisions arXiv:1707.02452 [math.AC] Author: M. Ceria

In preparation

Book
Bits, bytes and friends Authors: M. Ceria, G. Rinaldo and M. Sala

Paper
A performance-based approach to compare the Blockchain consensus procedures: PoW vs PoS vs Pure PoS. Authors: C. Lepore, M.Ceria, A. Visconti, U. Pratap Rao, K. Arvindbhai Shah, and L. Zanolini

Paper
Half error locator polynomials for efficient decoding of binary cyclic codes Authors: M. Ceria.

Paper
Bar Code and Janet-like division Author: M. Ceria

Paper
Combinatorics of ideals of points: a Cerlienco-Mureddu-like approach for an iterative lex game. Authors: M. Ceria, T. Mora

Paper
Towards involutive bases for effective algebras, Authors: M. Ceria, probably in cooperation with T. Mora

Paper
A variant of the iterative Moeller algorithm for giving Pommaret basis and its factorization, Author: M. Ceria

Distributed software

2012
JMBTest.lib: a J-marked basis tester Library available from Singular 3-1-6: `https://www.singular.uni-kl.de/index.php/singular-download.html` Author: M. Ceria

2012
JMSConst.lib: a J-marked schemes contructor Library available from Singular 3-1-6: `https://www.singular.uni-kl.de/index.php/singular-download.htmll` Author: M. Ceria

Submitted software

AffMarkedSchemes.lib Prototype library for Singular which performs Affine Marked Schemes computation. *Submitted to Singular Team.* Author: M. Ceria

Organized Conferences

ACA2020
Session organizer (with T.Mora and A- Leroy) of the session Effective Ideal Theory in Commutative and non-Commutative Rings and its Applications. Athens, July 15-18 2020.

Widecom2019
Local Chair and member of the Technical Commitee for the conference Widecom2019 - 11-13 February 2019

One-day workshops
As assistant of Prof. M. Sala, I contributed to the organization of

- the one-day workshop on *Blockchain and Innovative Applications*, 10/02/2017
- the one-day workshop on *Cryptographic Aspects of Cloud and Distributed Computing*, 28/10/2016

MEGA 2015
As assistant of Prof. M. Sala, I contributed to the local organization of the international conference MEGA 2015, University of Trento, Italy; June 15 – 19, 2015.

Miniworkshop *Coding Theory and Cryptography*
Organization of the miniworkshop *Coding Theory and Cryptography*, 13th and 14th October 2014, University of Turin. In collaboration with Doctor Chiara Marcolla (University of Trento).

Visiting

Neuchâtel
10-12-2019 – 13-12-2019 I have been invited to University of Neuchâtel by Prof. E. Gorla for research purpose and for delivering two seminars, one for the *research seminar on coding theory and cryptography* and the second for the *algebra seminar* (joint with Freiburg).

Rennes
26-08-2019 – 30-08-2019 Participation (completely funded) to the project WINE3 Workshop - Women in Numbers Europe 3 (3rd edition of the European WIN Workshop) In particular participation to the project by E. Byrne (University College Dublin) & R. Jurrius (The Netherlands Defense Academy) Title: q-Analogues in Combinatorics.

Linz
10-12-2018 – 15-12-2018 Invited for a seminar and for research purpose to the University of Linz by Prof. M. Kauers.

Kaiserslautern
During the period May-November 2012, I made short visits to *University of Kaiserslautern* (Germany) and worked with Prof. W. Decker and H. Schoenemann. I implemented two libraries for the software Singular, which have been integrated in version 3-1-6 of the software. `http://www.singular.uni-kl.de/index.php/singular-devteams.html`. Moreover, I followed some courses on computational algebraic geometry.

Referee (from 22-09-2016 on)

Journals and conferences
I have been a referee for the journals *AAECC* (Applicable Algebra in Engineering, Communication and Computing), *JSC* (Journal of Symbolic Computation), Mathematische Nachrichten, Advances in Mathematics of Communications, Security and Communication Networks, Theoretical Computer Science and Internet of Things: Engineering Cyber Physical Human Systems; moreover I have been a referee for the conferences *ISSAC* (International Symposium on Symbolic and Algebraic Computation), *MEGA* (International conference On Effective Methods in Algebraic Geometry) and *WTSC* (Workshop on Trusted Smart Contracts).

Reviews

Zentralblatt Math · **2012-Today**
5 reviewed papers.

Mathematical Reviews · **2017-Today**
2 reviewed papers.

Research groups

European Women in Mathematics (2019 -)

UMI · **National Mathematical Union (2018 -)**

De Componendis Cifris · **National association in Cryptography (Autum 2017 -)**

GNSAGA · **National Group for Algebraic and Geometrical structures and their Applications (2012 -)**

References

Prof. T. Mora
University of Genoa - 5919@unige.it

Prof. B. Buchberger
Research Institute for Symbolic Computation (RISC) Johannes Kepler University - bruno.buchberger@risc.jku.at

Students

Bachelor
Thesis co-advisor for six students with Prof. A. Visconti. External advisor with Prof T. Mora for two students.

Master
Master Thesis co-advisor for five students with Prof. M. Sala (one in collaboration with Dr. J. Shokrollahi of Bosh GmbH); Master Thesis co-advisor for one student with Dr. G. Rinaldo and for a student with Professor A. Visconti.

Tutoring 10-04-2015 — 25-04-2018
I have been tutor of 14 students, studying in the Major *Coding Theory and Cryptography* (now called *Cryptography*) of the Master of Degree in Mathematics at University of Trento, helping them with their study plans, average grade and in deciding about their internships in companies.

Conferences, Schools, Seminars (invited speaker)

Seminar · **9 April 2020**
Invited for a seminar (online, in French) at the *séminaire Mathématiques Discrètes, Codes et Cryptographie*, University of Paris 8.
Title: *Bases de Gröbner, degroebnerisation et leurs applications à la théorie des codes et à la cryptographie*

Seminars · **10-13 December 2019**
University of Neuchâtel. Title of the seminar [1]: *Half error locator polynomials for efficient decoding of binary cyclic codes.* Title of the seminar [2]: *Combinatorics of ideals of points: Groebner escaliers, separator polynomials and applications to Algebraic Statistics*.

Seminar · **8 November 2019**
I have been invited by Prof. Ulmer at University of Rennes for a seminar. Title of the seminar: *Half error locator polynomials for efficient decoding of binary cyclic codes.*
`https://irmar.univ-rennes1.fr/seminaire/genre/geometrie-et-algebre-effectives`

Seminar · **6 June 2019**

Invited by University of Milano Bicocca. Title of the talk: *Efficient computation of square-free separator polynomials and applications to algebraic statistics.*.
`https://www.matapp.unimib.it/it/eventi/efficient-computation-squarefree-separator-polynomials-and-applications-algebraic-statistics`

Seminar · **13 December 2018**
Invited by University of Linz. Title of the talk: *DIY for Groebner bases: multivariate Ore extensions and effective rings*. `http://www.algebra.uni-linz.ac.at/talks/schedule.php`

Seminar · **5 December 2018**

Invited by University of Genoa. Title of the talk: *DIY for Groebner bases: multivariate Ore extensions*. `https://commalge.tumblr.com /post/180718172787/algebrageometry-seminar`

Seminar · **4 December 2018**

Invited by University of Genoa. Title of the talk: *Bitcoin, blockchain and their applications*.

Seminar · **21 and 23 May 2018**

Invited by University of Genoa. Title of the talks: *A crash course in Bitcoin and Blockchain [part 1 and 2]*.

Seminar · **27 March 2018**
Invited by CTI Liguria for a seminar at Palazzo Ducale, Genoa. Title of the talk: *La crittografia dietro Bitcoin e blockchain*.

Seminar · **20 December 2017**
Invited for a seminar at University of Genoa. Title of the talk: *Combinatorics of involutive divisions*.

Seminar · **19 December 2017**
Invited for a seminar at University of Genoa. Title of the talk: *Bitcoin, Blockchain e loro Applicazioni*.

Conference · **26-27 October 2017**
Invited speaker to the *2nd Number Theory Meeting - Turin*, Polytechnic of Turin Title of the seminar: *Groebner bases and ECDLP: Involution*.
`http://ntmeeting.polito.it/2nd_Number_Theory_Meeting.html`

Conference · **29-30 May 2017** ·
Invited speaker at *Theory and Computation in Algebra and Algebraic Geometry with a dedication to Paolo Valabrega on the occasion of his 70(+2)th Birthday*, University of Turin
Title of the talk: *Combinatorics of involutive divisions*
`http://www.theoryandcomputation.unito.it/node/4`

Conference · **4-7 June 2014** ·
Invited speaker at the conference *Giornate di Geometria Algebrica e Argomenti Correlati XII*, Salone d'Onore del Castello del Valentino, Turin.
Title of the talk: *Basi involutive"Term-ordering free"* (Term-ordering free involutive bases).
`http://ricerca.mat.uniroma3.it/users/lopez/GGAACXII/Conferenzieri.html`

Conferences, Schools, Seminars (speaker/poster)

Conference · **2-7 September 2019**
Speaker at *Congresso UMI* - Pavia, Italy. Title of the talk: *Bar Code: a visual representation for finite sets of terms and its applications* `http://umi.dm.unibo.it/congresso2019/`

Conference · **16-20 July 2019**
Speaker at *ACA 2019* - Montréal, Canada. Title of the talk [1]: *Bar Code and Janet-like division* Title of the talk [2]: *HELP: the knight gambit for efficient decoding of BCH codes*
`http://aca2019.etsmtl.ca/`

Conference · **24-27 June 2019**
Speaker at *NCRA VI* - Lens, France. Title of the talk: *Why you should not even think to use Ore algebras in Cryptography* `http://leroy.perso.math.cnrs.fr/Congres2019/Main2019.HTML`

Conference · **16-21 June 2019**
Poster presentation at *MEGA2019* - Madrid, Spain. Title of the poster: *Combinatorial decompositions for monomial ideals* `http://eventos.ucm.es/12097/detail/mega-2019.html`

Conference · **15-20 April 2019** ·
Speaker at *PCA2019* - St.Petersburg, Russia. Title of the talk: *Applications of Bar Code to involutive divisions and a greedy algorithm for complete sets.* `https://pca-pdmi.ru/2019/`

Conference · **11-13 February 2019** ·
Tutorial Speaker at *Widecom2019* - Milan, Italy. Title of the talk: *Efficient cryptographic algorithms for securing passwords.*
`http://www.widecomconference.org/nsittest.co.nf/index.html`

Summer School · **August 2018**
Partecipation to the poster session of *AEC 2018* - RISC, Linz, Austria. Title of the poster: *Combinatorics of ideals of points: a Cerlienco-Mureddu-like approach for an iterative lex game.*

Conference · **24-27 July 2018**
Partecipation as speaker to *ICMS 2018* - Notre Dame, Indiana, USA. Title of the talk: *Efficient computation of squarefree separator polynomials.*
`http://icms-conference.org/2018/ICMS2018Schedule.pdf`

Conference · **18-22 June 2018**
Partecipation as speaker to *ACA 2018 - session Algorithms for zero-dimensional ideals* - Santiago de Compostela – Spain. Title of the talk: *Combinatorics of ideals of points: a Cerlienco-Mureddu-like approach for an iterative lex game.*
`https://www.unilim.fr/pages_perso/vincent.neiger/aca18/`

Conference · **2-7 April 2018**
Participant to the poster session of the conference *Symmetry and Computation*, CIRM - Luminy - Marseille. Title of the poster: *Combinatorics of involutive divisions*
`https://www.cirm-math.fr/ProgWeebly/Renc1772/Prog1772.pdf`

Seminar · **September 2017**
Findomestic, Florence. Lecturer of a seminar titled: *Introduzione alla tecnologia blockchain ed alle sue principali applicazioni* (Introduction to blockchain technology and its main applications).

Conference · **12-16 June 2017**
Partecipation as speaker to *MEGA 2017. Effective methods in Algebraic Geometry*, University of Nice, France. Title of the talk: *Bar Code for monomial ideals*
`https://mega2017.inria.fr/`

Seminar · **4 November 2016**
Speaker to the miniworkshop *Seminari di Teoria dei Numeri* Title of the seminar: *Half Error Locator Polynomial for binary cyclic codes*.
`https://www.dipmatematica.unito.it/do/home.pl/View?doc=teorianumeri.html`

Seminar · **April 2016**
SGS, Verona Lecturer of a seminar titled: *E-Voting e Blockchain*.

Seminar · **May 2016** ·
Polytechnic of Turin Title of the talk: *Crittografia e sicurezza del sistema Bancomat* (Cryptography and security of the Bancomat system).

Summer School · **July 2015** ·
Partecipation to the poster session of the summer school *AEC, 2nd Algorithmic and Enumerative Combinatorics Summer School 2015* Title of the poster: *Bar Codes and Strongly Stable Ideals* . Participation to the summer school.

Summer School and Conference · **1 - 10 July 2015**
Speaker at the conference *Current Trends on Groebner Bases*, Osaka, Japan. Title of the talk: *A unifying form for noetherian polynomial reductions*.Funded by INdAM. Participation to the summer school.

Miniworkshop · **13-14 October 2014**
Speaker at the miniworkshop *Coding Theory and Cryptography*, Department of Mathematics, University of Turin. Title of the talk: *Polinomi locatori sparsi per codici ciclici binari* (Sparse locator polynomials for binary cyclic codes).
`https://www.unito.it/eventi/mi niworkshop-coding-theory-and-cryptography`

Seminar · **April 2014**
Polytechnic of Turin. Title of the talk: *Basi involutive"Term-ordering free"* (Term-ordering free involutive bases).

Conference · **3- 7 June 2013**
Partecipation to the poster session of the convention *MEGA 2013. Effective methods in Algebraic Geometry*, University of Frankfurt, Germany. Title of the poster: *JMBTest.lib and JMSConst.lib: Singular Tools for J-Marked Schemes*.
`https://www.math.uni-frankfurt.de/mega2013/program.shtml`

Summer School · **24-28 June 2013**
EACA'S Second International School On Computer Algebra and Applications, University of Valladolid, Spain. Lecturer of a seminar titled: *Bar-codes for monomial ideals*. Partecipation to courses.

Seminar · **December 2012**
Polytechnic of Turin Title of the talk: *L'Asse del Male* (The Axis-of-Evil Theorem).

Summer School · **1-13 October 2012**
Algebra for Secure and Reliable Communication Modeling, Institute of Physics and Mathematics of the University of Michoacán, Messico. Lecturer of a seminar titled: *The Axis-of-Evil Theorem*. Partecipation to courses.

Conference · **17-21 September 2012**
Partecipation as a speaker to the convention *MAP 2012 - Mathematics, Algorithms and Proofs*, University of Konstanz, Germany. Title of the seminar: *The Axis-of-Evil algorithm*. Partecipation to the 'Young Researchers' Session' with a brief talk on my research activities. `https://cms.uni-konstanz.de/fi leadmin/archive/map2012/schedule-and-slides/index.html`

Summer School · **July-August 2012**
PHD School on Groebner Bases, Curves, Codes and Cryptography, University of Trento. Lecturer of a seminar titled: *A Bar-Code algorithm for the 'Axis of Evil' Theorem*. Partecipation to courses.

Summer school · **October 2011**
International School on Computational Commutative Algebra and Algebraic Geometry, Villa Pace-University of Messina. Lecturer of a seminar titled: *Classification of Adjoint Curves*. Partecipation to courses.

Followed Conferences and Schools

Conference · **June 2017**
Fq13 - The 13th International Conference on Finite Fields and their Applications, Gaeta.

Conference · **April 2015**
The Ninth International Workshop on Coding and Cryptography 2015 , Paris.

Conference · **March 2012**
Geometria delle varietà algebriche in honour of Professor A.Conte, Department of Mathematics, University of Turin.

Conference · **April 2011**
Partecipation to the *Commutative Days in Turin, a meeting in honour of Silvio Greco on the occasion of his 70th birthday*, Department of Mathematics, Polytechnic of Turin.

Conference · **October 2011**
Partecipation to the Mathematica 5^{th} User Group Meeting, Department of Mathematics, University of Turin.

Teaching Experience - University courses

18.09.2017 - 16.02.2018 ·
Master Degree in Mathematics · Lecturer for the Advanced Coding Theory and Cryptography course taught on the second year of the Master Degree in Mathematics, Major in Coding Theory and Cryptography, University of Trento. Professor: M. *Sala*.

14.09.2015 - 12.02.2016 and 14.09.2016 - 17.02.2017 ·
Master Degree in Mathematics · Lecturer for the Algebraic Cryptography course taught on the first year of the Master Degree in Mathematics, Major in Coding Theory and Cryptography, University of Trento Professor: M. *Sala*.

2016
PhD in Mathematics Assistant Lecturer for the PhD course *Groebner Bases applied to Cryptography and Coding Theory*, University of Trento Professor: M. *Sala*.
`https://www.unitn.it/drmath/43/manifesto-studies` (see Manifesto 2015/2016)

2013–2014 ·
Bachelor in Engineering Lecturer for the Geometry course taught on the first year of the bachelor in Engineering, Politecnico di Torino. Professor: G. *Casnati*.

2011–2013 ·
Bachelor in Engineering Lecturer for the Geometry course taught on the first year of the bachelor in Engineering, Politecnico di Torino. Professor: C. *Massaza*.

Teaching Experience - courses for professionals

May 2018
Lecturer for the course *Post-Quantum Cryptography* for the part on multivariate post-quantum cryptography. Scientific coordination: M. *Sala*.

November 2017
Lecturer for the course *Monero: the dark side of cryptocurrencies* Professor: M. *Sala*.

October 2017 ·
Lecturer for the course *Bitcoin, Blockchain and their new frontiers in Milan* Professor: M. *Sala*.

May 2017 ·
Lecturer for the course *Bitcoin, Blockchain and their new frontiers in Trento* Professor: Prof. M. *Sala*.

November 2016
Assistant Lecturer for the courses *Bitcoin, Blockchain and their new frontiers in Milan*, *Bitcoin, Blockchain and their new frontiers in Rome*. Professor: M. *Sala*.

September 2016 ·
Assistant Lecturer for the course *Bitcoin, Blockchain and their new frontiers II*, University of Trento Professor: M. *Sala*.

May 2016 - May 2017 ·
Assistant Lecturer for the course *Bitcoin, Blockchain and their new frontiers*, University of Trento Professor: M. *Sala*.

Teaching Experience - e-learning and courses' coordination

Course coordination *2018/2019* ·
Coordination (*Professore a contratto*) for the blended course in Computer Science for the faculty of Linguistic Mediation.

E-learning *2015 - 2018*
I assisted Prof. Massimiliano Sala in the preparation of the teaching matherial and in the organization of the two one-day face-to-face events of the EIT online course *Applications of Cryptography to Security and Privacy* and in the preparation of the teaching matherial for the online course *BoAB: Bitcoin and other Applications of Blockchain*. I have maintained the online platform of the latter course and done the tutoring for the participants until April 2018.

Teaching Experience - experience at school

November 2014
Liceo Istituto Comprensivo S. Francesco d'Assisi – Biella · Brief mathematics substitute teaching.

Summer 2014
Liceo Giuseppe & Quintino Sella – Classico Linguistico Artistico · Mathematics recovery course.

Education

2011-2013 · **University of Turin, Italy**
PhD in Mathematics, XXVI cycle, University of Turin. · Scientific field MAT02-Algebra.
PhD degree obtained on 14/02/2014 (University of Turin).
Title of PhD Thesis: *Combinatorial structure of monomial ideals.*
Description: In the thesis we study *monomial ideals* from a combinatorial point of view, mainly dealing with their Groebner escalier. Many links with coding theory and enumerative combinatorics are provided. Moreover, the code of some related software is attached to the thesis.
Developed with Professors: M.G. *Marinari*, T. *Mora*, M. *Roggero*.

2007-2010 · **University of Turin, Italy**
Master degree in Mathematics · Class: 45/S (class of Mathematics Masters of Science, D.M. 509/1999), Faculty of Mathematical, Physical and Natural Science, University of Turin Master degree obtained on 20/07/2010 with grade 110/110 cum laude and mention.
Title of MSc Thesis: *Conductor and adjoints of algebraic curves.*
Description: The thesis focuses on the several definitions of *adjoint curve*, distinguishing them and highlighting their reciprocal relationships. Additionally, a software classifying adjoint curves is developed and its pseudocode attached to the thesis, with some significant examples.
Developed with Professors: M. *Roggero* and P. *Valabrega*.

2003-2007 · **University of Turin, Italy** ·
Bachelor degree in Mathematics · Faculty of Mathematical, Physical and Natural Science, University of Turin · Bachelor degree obtained on 27/04/ 2007 with grade 104/110.
Title of Bachelor Thesis: *Matroids and parking functions.*
Description: This thesis deals with graph theory and, more precisely, with the theory of *matroids*. After a theoretical overview, it gives a practical application, examining its connection with *parking functions*.
Developed with Professor M. *Roggero*.

Foreign languages

Italian
Mothertongue

English
Good
International English Language Testing System (Academic), got in September 2010 with grade 7.

French
Scholastic; B1 MC Graw Hill certificate got online

Japanese
Scholastic

Software Development Skills

OS
- Linux (Ubuntu)
- Microsoft Windows
- Mac OS X
- Android

Programming
- C/C++ (basic notions)
- Singular
- Magma

Softwares
- Singular
- Cocoa
- Maple
- Magma
- Microsoft Office
- Outlook
- Thunderbird
- Internet Explorer
- Mozilla Firefox
- Chrome/Chromium
- Safari
- Adobe reader
- Opera

E-learning
- Moodle
- Sakai
- Google Classroom

Other information

Advisory Board
I contributed to the creation of an *Advisory Board* of companies in Trento. These companies financed stages and scholarships for students and iterfaced with the Department, higlighting the specific knowledge they would need for people to work within them.

Hopf Algebras course
followed the Hopf algebra Course held by Prof. Ardizzoni to the PhD School in Mathematics at University of Turin.

Lie Algebras course
followed the Lie algebra Course held by Prof. De Graaf to the PhD School in Mathematics at University of Trento.

Researchers' night
I participated to the italian researcher's night both in Turin and in Trento.

MICHELA CERIA - RESEARCH STATEMENT

My main research areas concern the combinatorial aspects of Computational Algebra and the theory of commutative and noncommutative Groebner bases. These topics present several applications, for example in the framework of Coding Theory, Cryptography and Algebraic Statistics.

1. Introduction for non-specialist audience

Solving polynomial equation systems is an important problem, having applications to different science fields. The standard tools for "solving" are Groebner bases, a "smart rewriting" for systems, making them simpler to solve. There is not only one Groebner basis for a system and some of the possible bases can be more efficient to find. The best such bases are the involutive bases, also applied in the study of partial differential equations. One can set an "analysis-algebra dictionary", translating PDEs into polynomial equations, manipulating them via involutive bases and finally coming back to the PDEs' framework to get the solution. In a similar fashion, Groebner bases have been generalized to some differential algebras as Weyl algebras or Ore algebras, to study their structure. As a drawback, Groebner bases are computationally heavy to find. On the other side, what happens is that for many applications, *it is not necessary to use Groebner bases*. Therefore, the Grobner-free solving, expressed and sponsored in Mora's books, proposes to find alternative ways to get the same solutions, using, for example, tools from linear algebra and combinatorics. Combinatorics can be used to study the reverse problem with respect to "solving", the "bonding problem for algebras and ideals". Indeed, given the variety associated to a 0-dimensional ideal, the rich structure of the quotient algebra can be recovered using only combinatorics. My research is mainly focused on the study of tools for degroebnerizing problems on polynomial/monomial ideals, both in the commutative and noncommutative case, and of their applications.

2. Research proposal

An important tool for Degroebnerization is the main result of my thesis: a compact and visual representation of monomials, the Bar Code, which allows to read many properties of monomial ideals. Among its potential uses, I have applied Bar Codes as a tool for the study of Janet and Janet-like divisions. One of my aims of research is to investigate further on applications of Bar Code in the involutive setting, as the computation of Pommaret's bases and their factorization in the case of 0-dimensional radical ideals and by means of interpolation. Solving polynomial equations systems is a deeply studied problem, with many applications in several scientific fields of study. Groebner bases have been developed for this scope. One of the aims of my future research is to study the reversed problem, i.e. the bonding problem: given a finite set X of points or abstract functionals, describe the algebra representing such a set, i.e. A=P/I, the quotient of the polynomial ring P modulo the ideal I consisting of all polynomials vanishing at X. The structure of A=P/I is suitable to be studied with combinatorial arguments, deeply used in the case of I radical. We intend to propose a general Degroebnerized framework, where to efficiently solve combinatorically the main problems (membership and normal form computations, separators, etc.) surely for 0-dimensional radical ideals but, potentially, also in a more general setting. This has applications, as an example, to coding theory, reverse engineering and algebraic statistics. Much has still to be studied in this context, once relaxed the radicality hypothesis on I. It would be fundamental to systematize Macaulay's results and extend his theory to points with multiplicity and abstract functionals. Another important point is the study of what can be generalized to the noncommutative case, first to the Poincaré-Birkhoff-Witt case and then to the more complex case of free algebras. The many factorizations on Ore Algebras

and so the existence of too many roots as expected via Hilbert function create a difficult problem for a combinatorial approach.

The idea of decoding a cyclic code C by means of Groebner bases has been introduced in the Ninetees and much literature followed this path. An ideal I is associated to C and its lexicographical Groebner basis G allows to decode each received word to get the message. The basis contains Sala-Orsini general error locator polynomial (GELP), whose roots are the error locations, once evaluated in the syndromes desumed from the received word. Computing this basis has double-exponential complexity in the number of variables and the GELP may be a dense polynomial, so evaluation may be inefficient. Therefore, an important problem for the theory of cyclic codes is to compute efficiently a sparse locator polynomial. We propose a new approach to find such a sparse polynomial. In particular, we will compute a locator polynomial, descending from the GELP, without needing the computation of a Groebner basis, looking for sparse solutions of the problem from the case of error correction capability of at most 2, for binary cyclic codes. We will use the results on bonding: instead of taking the syndrome ideal I and computing a Groebner basis, we will consider the syndrome variety $V = V(I)$ and interpolate on it to find the locator. Starting from the variety allows a preliminary combinatorial study of the associated lexicographical Groebner escalier, enabling to halve the number of points of the variety needed to interpolate. Moreover, only one factor of the GELP is needed: the half error locator polynomial (HELP), whose roots (again once evaluated in the syndromes) are half of the error locations, while it is easy to deduce the other half by a linear relation.

As regards reverse engineering, recently we extended the previous combinatorial algorithms for computing the lexicographical Groebner escalier of 0-dimensional (radical) ideals, proposing an efficient iterative but non-inductive procedure which in particular produces the separators of the given points, used in reverse engineering for gene regulatory networks.

As regards algebraic statistics, separator polynomials are building blocks for constructing the indicator function, used to study fractions of full factorial designs. An early-stage research in Algebraic Statistics is related to coloured probability tree models, aimed to study conditional independence among events by posing them in suitable trees. I aim to cooperate with E. Riccomagno (University of Genoa) to the combinatorial study of such trees.

In the context of noncommutative Groebner bases, we introduced the notion of Weispfenning multiplication, which allowed us to "commutivize" the computation of restricted bilateral ideals and give a more efficient alternative to Mora's algorithm for computing Groebner bases over any effective ring. We are working to extend to effective algebras the theory of weak involutive bases and see how to reformulate the procedure to extend involutive bases to effective rings defined over principal ideal domains.

Here is a cryptographic application of our studies on noncommutative Groebner bases. Indeed, graded Ore extensions can be employed in the construction of cryptographic protocols. Burger-Heinle proposed a Diffie-Hellman like protocol over multivariate Ore extensions. The two communicating parties, Alice and Bob, agree on a multivariate Ore extension T with constant subring R. Then they choose three non-central elements L,P,Q in T (non-mutually commuting) and two subsets Cl, Cr of T whose elements do not commute with L. The elements in Cl (Cr) commute among them. All these data are public. Alice (resp. Bob) picks secretly (P_A, Q_A) (resp. (P_B, Q_B) in ClXCr. Alice sends Bob $A = P_A L Q_A$ and receives $B = P_B L Q_B$ from him: the shared secret is

$$P_A B Q_A = P_A P_B L Q_B Q_A = P_B P_A L Q_A Q_B = P_B A Q_B.$$

While generalizing this protocol to iterated Ore extensions with power substitutions, we made a cryptanalysis based on reduction and right/left division.

This summer, I had the opportunity to participate to the workshop WINE3 (Women in Numbers Europe 3). I worked in the group project titled *q-Analogues in Combinatorics*. In this period, I wrote with the team of WINE3 a paper, which has been submitted to a referenced proceedings based on the project. After this experience, I hope I will have the opportunity to continue cooperating with this group.

Data 13/04/2020 Luogo Biella