ALBERT GARRETA

I am a mathematician and computer scientist (Ph.D.). I began my career researching algorithmic problems in algebra and discrete optimization. Later I became interested in other areas such as machine learning, and cryptography and blockchain technology.

CONTACT

- garreta.a@gmail.com
- Bilbao, Spain
- homepage
- Github
- Google scholar profile
- Kaggle profile

KEYWORDS

- Algorithmic problems in rings, groups, etc.
- Machine learning
- Cryptography
- Blockchain technology and development

PROGRAMMING SKILLS

Python
Solidity
Cairo
Rust
C++
LaTeX

LANGUAGES

English
Spanish
Catalan

ACADEMIC APPOINTMENTS

07/2021 - today
BCAM Basque Center of Applied Mathematics, Bilbao (Spain)
Postdoctoral Researcher

01/2017 - 07/2021
University of the Basque Country, Bilbao (Spain)
Postdoctoral Researcher

EDUCATION

08/2012 - 12/2016
Stevens Institute of Technology, New Jersey (USA)
PhD in Mathematics
Received an **excellence in graduate research award**

09/2007 - 07/2012
Polytechnic University of Catalonia, Barcelona (Spain)
Licenciature in Mathematics
Roughly equivalent to what currently is a 4-year college degree and a 1-year master's degree

SELECTED WORK AND ACHIEVEMENTS

- Publication of mathematical and computer science papers at top ranked journals. E.g. in Bulletin of Mathematical Sciencies, **ranked 17 out of 325** in the category of Mathematics (JCR criterion).
- **9th out of 1089** solution to the machine learning competition Photometric LSST Astronomical Time-series Classification Challenge (PLAsTiCC).
- **3rd place solution** at the first StarkNet hackathon (Amsterdam, 2022). Starknet is a Layer 2 network that uses **zero-knowledge proofs** to scale the Ethereum network. Repository
- **Honorable mention** at the Underhanded Cairo Contest (this contest had a total of 1 winner and 2 honorable mentions). The goal was to create a piece of Cairo code that looks harmless but that contains an exploit. Repository
- Cryptography teaching and theses direction for the Master's degree Blockchain Technology and Crypto-Economy (link in Spanish).

SKILLS OVERVIEW

Commutative and non-commutative algebra | Group and semigroup theory | Logic | Number theory

Computational complexity | Algorithms | Cryptography | Zero knowledge proofs | Group-based cryptography

Machine learning | Deep leaning | Reinforcement learning | Statistical inference

Blockchain technology and development | EVM-compatible networks | StarkNet and Cairo

Python | Solidity | Cairo | Rust | LaTeX

Technical writing | Research presentation and divulgation | Self-learning

PUBLICATIONS

13. A decentralized private data marketplace using blockchain and secure multi-party computation
with Julen Bernabé and Oscar Lage

2022 **submitted for revision** preprint

12. Group equations with abelian predicates
with Laura Ciobanu

2022 **submitted for revision** preprint

11. Solving word equations with Monte Carlo Tree Search and black-box solvers
Albert Garreta

2021 **submitted for revision** preprint

10. Diophantine problems in rings and algebras: undecidability and reductions to rings of algebraic integers
with Alexei Miasnikov and Denis Ovchinnikov

2021 **submitted for revision** arXiv

9. Results of the Photometric LSST Astronomical Time-series Classification Challenge (PLAsTiCC)
with Renee Hlozek et al.

2022 **to appear in The Astrophysical Journal Supplement** preprint

8. Simple groups with infinite verbal width and the same positive theory as free groups
with Montserrat Casals-Ruiz, Ilya Kazachkov, and Javier de la Nuez

2021 **to appear in Israel Journal of Mathematics** arXiv

7. On equations and first-order theory of one-relator monoids
with Robert D. Gray

2021 **Information & Computation, vol. 281, 104745, ISSN 0890-5401, 44 pages** doi, arXiv

6. On the positive theory of groups acting on trees
with Montserrat Casals-Ruiz, and Javier de la Nuez

2021 **International Math. Research Notices (IMRN), vol. 2021, no. 3, 44 pp. 1837–1918** doi, arXiv

5. Metabelian groups: full-rank presentations, randomness and Diophantine problems
with Leire Legarreta, Alexei Miasnikov, and Denis Ovchinnikov

2021 **Journal of Group Theory, vol. 24, no. 3, pp. 453-466** doi, arXiv

4. Diophantine problems in solvable groups
with Alexei Miasnikov and Denis Ovchinnikov

2020 **Bulletin of Mathematical Sciences, v. 10 (1) (2020), pp. 1-21** doi, arXiv

3. Full rank presentations and nilpotent groups: structure, Diophantine problem, and genericity
with Alexei Miasnikov and Denis Ovchinnikov

2020 **Journal of Algebra, v. 556 (2020), pp. 1-34** doi, arXiv

2. Engel elements in some fractal groups
with Gustavo Fernández-Alcober and Marialaura Noce

2018 **Journal of Group Theory, vol. 24, no. 3, pp. 453-466** doi, arXiv

1. Random nilpotent groups, polycyclic presentations, and Diophantine problems
with Alexei Miasnikov and Denis Ovchinnikov

2017 **Groups Complexity Cryptology, v. 9 (2) (2017), pp. 99-115** doi, arXiv

ARTICLES IN PREPARATION

Regressing bone age from radiographs via interpretable features
with Jordi Fortuny, Oscar Gasulla, Ferran Mazaira, and Miguel Teixidó

Studying the Diophantine problem in finitely generated rings via bilinear maps
with Alexei Miasnikov and Denis Ovchinnikov

Equations in polycyclic groups
with Alexei Miasnikov and Denis Ovchinnikov

BLOCKCHAIN

3rd place solution of the first StarkNet Hackathon (Amsterdam, 2022). Repository.
Starknet is a Layer 2 network that uses zero-knowledge proofs to scale Ethereum.

Honorable mention at the Underhanded Cairo Contest
This contest had a total of 1 winner and 2 honorable mentions. The goal was to create a piece of Cairo code that looks harmless but that contains an exploit. Cairo is a programming language dedicated to zero-knowledge proofs. Repository

MACHINE LEARNING COMPETITIONS

Photometric LSST Astronomical Time-series Classification Challenge (PLAsTiCC)
2018 Top 1% position (9th out of 1094) link

Abstraction and Reasoning Challenge
2021 Top 8% position (66th out of 914) link

Costa Rican Household Poverty Level Prediction
2018 Top 18% position (106th out of 619) link

THESES SUPERVISED

SMPC & BLOCKCHAIN: Creating Private Data Marketplaces
Julen Bernabé (supervised by Albert Garreta and Oscar Lage)
2021 **Blockchain Technology and Crypto-economy (Master's Degree)** link

Blockchain Homomorphic Encryption
Leire Etxebarria (supervised by Albert Garreta and Oscar Lage)
2021 **Blockchain Technology and Crypto-economy (Master's Degree)** link

TEACHING

Modern Cryptography
Blockchain Technology and Crypto-economy (Master's Degree)
Q1 and Q2 of 2022 University of the Basque Country, Bilbao (Spain)

Foundations of Cryptography
Blockchain Technology and Crypto-economy (Master's Degree)
Q3 and Q4 of 2021 University of the Basque Country, Bilbao (Spain)

Modern Cryptography
Blockchain Technology and Crypto-economy (Master's Degree)
Q1 and Q2 of 2021 University of the Basque Country, Bilbao (Spain)

Foundations of Cryptography

Blockchain Technology and Crypto-economy (Master's Degree)

Q3 and Q4 of 2020 University of the Basque Country, Bilbao (Spain)

Introduction to Deep Learning

5h PhD Course

Q4 of 2020 University of the Basque Country, Bilbao (Spain)

Data Science and python programming

Bachelor of Business Administration

Q3 and Q4 of 2019 ESADE, Barcelona, Spain

Differential Equations, Multivariable Calculus

Several undergraduate courses (around 500 hours in total)

2012-2016 Stevens Institute of Technology, Hoboken, (New Jersey, USA)

INVITED TALKS AT CONFERENCES

1. Geometric and Asymptotic Group Theory with Applications, Edinburgh (UK), (GAGTA)2021, talk link
2. Groups and Topological Groups, Cetara (Italy), 2019
3. Dagstuhl Seminar 'Algorithmic Problems in Group Theory', Schloss Dagstuhl (Germany), 2019
4. Biannual congress of the Royal Spanish Mathematical Society (special session), Santander (Spain), 2019
5. Fall Meeting of the American Mathematical Society (special session), Boston (USA), 2018
6. Joint meeting of the Edinburgh Math. Society and the Catalan Math Society, Edinburgh (UK), 2017
7. Eleventh Barcelona Weekend in Group Theory, Polytechnic University of Catalonia (Spain), 2016
8. Equations and Formal Languages in Algebra, Les Diablerets (Switzerland), 2016

CONTRIBUTED TALKS AT CONFERENCES

1. Russian Workshop on Complexity and Model Theory, Moscow (Russia), 2019
2. Advances in Group Theory and Applications, University of Lecce (Italy), 2017
3. Young Geometric and Asymptotic Group Theory with Applications, University of the Basque Country (Spain), 2017
4. Young Researchers Algebra Conference, University of Naples (Italy), 2017
5. Fall Meeting of the American Mathematical Society (special session), Bowdoin College, Maine (USA), 2016
6. Geometric and Asymptotic Group Theory with Applications (GAGTA), City College of NY (USA), 2015

ACADEMIC VISITS

1. Oberwolfach Research Institute for Mathematics (Germany), 2021 (Received **Research in Pairs Grant**)
2. Heriot-Watt University (Edinburgh, UK), 2019
3. University of East Anglia (Norwich, UK), 2019
4. Stevens Institute of Technology (New Jersey), 2019
5. Stevens Institute of Technology (New Jersey), 2018
6. University of Salerno (Italy), 2017

ORGANIZATION OF CONFERENCES AND SEMINARS

1. *Bilbao algebra seminar*, University of the Basque Country (Bilbao), 2016-2021, seminar link
2. *GTA Gran Bilbao 2*, University of the Basque Country (Bilbao), 2020, link
3. *Young Geometric Group Theory 8 (YGGT8)*, University of the Basque Country (Bilbao), 2019 link
4. *Geom. and Asymptotic Group Theory with Applications (GAGTA)*, Univ. of the Basque Country (Bilbao), 2017, link

GRANTS AND RESEARCH PROJECTS

1. MFO (Mathematisches Forschungsinstitut Oberwolfach) Research in Pairs Fellowship, 2020
2. European Research Council Starting Grant, PCG-336983. PI: I. Kazachkov, 2017-2021
3. Spanish government research project, MTM2017-86802-P: Groups and geometry. PI: G. Fernández, 2017-now
4. Basque government research project, IT974-16. PI: Ilya Kazachkov, 2018-now.