

# Corentin Le Coz

POST-DOC · PURE MATHEMATICS

Rue de la Célidée 25/72, 1080 Brussels, Belgium

☎ (+33) 6 74 87 42 73 | ✉ corentinlecoz@outlook.com | 🏠 users.ugent.be/ clecoz/

## Areas of research

---

I am interested in geometry and analysis in metric spaces, including Cayley and vertex-transitive graphs. More precisely, my research is focused on coarse-geometric monotone invariants: asymptotic dimension, Poincaré and separation profiles. Recently, I've also been interested in applications of geometric group theory in cryptography.

## Work Experience

---

### Gent Universiteit

Post-Doc

Supervisor: T. De Medts

*High-dimensional expanders, Building theory*

*Ghent, Belgium*

Oct 2022 - PRESENT

### Technion – Israel Institute of Technology

Post-Doc

Supervisor: N. Lazarovich

*Geometric group theory, Hyperbolic geometry*

*Haifa, Israel*

Nov. 2020 - Oct 2022

## Education

---

### Université Paris-Saclay

PHD IN PURE MATHEMATICS

Supervisors: R. Tessera (IMJ-PRG), J. Brioussell (IMAG)

PhD report available [here](#)

*Coarse geometry, Isoperimetry, Expansion of graphs*

*Orsay, France*

2017 - 2020

### ENS Paris-Saclay

MASTER'S DEGREE IN MATHEMATICAL TEACHING

Preparation for French higher education competitive exam

Diploma "agrégation" obtained in 2017, ranked 26<sup>th</sup> over 305 admitted.

NUMEN: 25E1732665SON

*Linear algebra, Calculus, Probability, Computer algebra*

*Cachan, France*

2016 - 2017

### Université Paris-Diderot

MASTERS DEGREE IN MATHEMATICAL RESEARCH

Master thesis: Integrable orbit equivalence and free groups, after Lewis Bowen

Supervisor: R. Tessera (IMJ-PRG)

*Measured group theory, Operator algebra, Differential Geometry*

*Paris, France*

2015 - 2016

### ESPCI

ENGINEERING TRAINING

Engineering internship: Protocol development for a TEM microscope, at Solvay

Worker internship: Catalyser crafting at Axens

*Crystallography, Chemistry, Electrical engineering*

*Paris, France*

2011 - 2014

## Patent

---

### Post-quantum Hash Function using Higher Dimensional Special Linear Groups

*Received by the USPTO*

CO-INVENTOR WITH C. BATTARBEE (YORK), R. FLORES (SEVILLA), T. KOBERDA (VIRGINIA) AND D. KAHROBAEI (CUNY)

*We define new families of Tillich-Zémor hash functions, using higher dimensional special linear groups over finite fields as platforms. The Cayley graphs of these groups combine fast mixing properties and high girth, which together give rise to good preimage and collision resistance of the corresponding hash functions. We justify the claim that the resulting hash functions are post-quantum secure.*

USPTO provisional application number 63/584,526.

## Publications

---

### Right-angled Artin groups and the cohomology basis graph

Submitted to the *Pac. J. Math.*

CO-AUTHOR WITH R. FLORES, D. KAHROBAEI AND T. KOBERDA

Let  $\Gamma$  be a finite graph and let  $A(\Gamma)$  be the corresponding right-angled Artin group. From an arbitrary basis  $\mathcal{B}$  of  $H^1(A(\Gamma), \mathbb{F})$  over an arbitrary field, we construct a natural graph  $\Gamma_{\mathcal{B}}$  from the cup product, called the cohomology basis graph. We show that  $\Gamma_{\mathcal{B}}$  always contains  $\Gamma$  as a subgraph. This provides an effective way to reconstruct the defining graph  $\Gamma$  from the cohomology of  $A(\Gamma)$ , to characterize the planarity of the defining graph from the algebra of  $A(\Gamma)$ , and to recover many other natural graph-theoretic invariants. We also investigate the behavior of the cohomology basis graph under passage to elementary subminors, and show that it is not well-behaved under edge contraction.

Preprint available on [arXiv.org](https://arxiv.org).

### Higher dimensional platforms for Tillich-Zémor hash functions

Submitted to *Adv. Math. Commun.*

MAIN AUTHOR, CO-AUTHOR WITH C. BATTARBEE, R. FLORES, T. KOBERDA AND D. KAHROBAEI

We define new families of Tillich-Zémor hash functions, using higher dimensional special linear groups over finite fields as platforms. The Cayley graphs of these groups combine fast mixing properties and high girth, which together give rise to good preimage and collision resistance of the corresponding hash functions. We justify the claim that the resulting hash functions are post-quantum secure.

Preprint available on [Cryptology ePrint Archive](https://eprint.iacr.org).

### Poincaré profiles of lamplighter diagonal products

Submitted to *Groups, Geom. Dyn.*

AUTHOR

We exhibit finitely generated groups with prescribed Poincaré profiles. It can be prescribed for functions between  $n/\log n$  and linear, and is sharp for functions at least  $n/\log \log n$ . As applications, we show that there exists bounded degrees graphs of asymptotic dimension one that do not coarsely embed in any finite product of bounded degrees trees, exhibit hyperfinite sequences of graphs of arbitrary large distortion in  $L^p$ -spaces, and prove the existence of a continuous family of pairwise uncomparable amenable groups.

Preprint available on [arXiv.org](https://arxiv.org)

### Hyperbolic groups with logarithmic separation profile

Accepted at *Algebr. Geom. Topol.*

CO-AUTHOR WITH N. LAZAROVICH

We prove that hyperbolic groups with logarithmic separation profiles split over cyclic groups. This shows that such groups can be inductively built from Fuchsian groups and free groups by amalgamations and HNN extensions over finite or virtually cyclic groups. However, we show that not all groups admitting such a hierarchy have logarithmic separation profile by providing an example of a surface amalgam over a cyclic group with superlogarithmic separation profile.

Preprint available on [arXiv.org](https://arxiv.org)

### Separation profiles, isoperimetry, growth and compression

published in *Ann. Inst. Fourier*

CO-AUTHOR WITH A. GOURNAY

We give lower and upper bounds for the separation profile (introduced by Benjamini, Schramm & Timár) for various graphs using isoperimetric profile, volume growth and Hilbertian compression. We show that solvable groups of exponential growth cannot have a separation profile bounded above by a sublinear power function. We also introduce a notion of local separation, with applications for percolation clusters of  $\mathbb{Z}^d$  and graphs which have polynomial isoperimetry and growth.

Publication available [here](#)

## Talks

---

06/23	<b>Magic square seminar</b> , Thick embeddings of finite graphs into Euclidean spaces	UGent, Belgium
05/23	<b>UGent-KULAK seminar</b> , Embeddings of the lamplighter group into solvable groups	Kortrijk, Belgium
04/23	<b>EOS seminar</b> , Thick embeddings of finite graphs into Euclidean spaces	UGent, Belgium
10/22	<b>EOS seminar</b> , Hyperbolic groups with logarithmic separation profile	UCL, Belgium
07/22	<b>Rosenthal's birthday conference</b> , Post-quantum hash functions using $SL_n(\mathbb{F}_p)$	Zurich, Switzerland
07/22	<b>Séminaire Darboux</b> , Groupes hyperboliques à profil de séparation logarithmique	Montpellier, France
03/22	<b>CUNY Algebra and Cryptography Seminar</b> , Hyperbolic groups with logarithmic separation profile	New York City, USA
07/21	<b>Young Geometric Group Theory X</b> , Embeddings into products of trees (lightning talk)	online
06/21	<b>GAGTA 21</b> , Poincaré profiles of diagonal products of lamplighters (contributed talk)	online
12/20	<b>Technion Geometry and Topology Seminar</b> , Expanders, Property (T) and Poincaré profiles	Haifa, Israel
06/20	<b>University of Bristol Analysis and Geometry Seminar</b> , Separation profiles of solvable groups	Bristol, UK
05/20	<b>ENS Group Theory Seminar</b> , Separation and isoperimetric profiles	Paris, France
02/20	<b>Alfréd Rényi Institute Geometry and Probability Seminar</b> , Separation and isoperimetric profiles	Budapest, Hungary
01/20	<b>Séminaire Darboux de l'Université de Montpellier</b> , Profil de séparation des groupes résolubles	Montpellier, France
05/19	<b>Séminaire GTD de l'Université Paris-Saclay</b> , Une étude des liens entre séparation et isopérimétrie	Orsay, France
03/19	<b>ANR GAMME</b> , Une étude des liens entre séparation et isopérimétrie	St Etienne, France
12/18	<b>Graduate students popularization seminar</b> , Growth function of groups	Orsay, France

## Conferences and workshops

---

09-12/24	<b>Post-Quantum Algebraic Cryptography</b> , IHP trimester (invited, to come)	Paris, France
04/24	<b>Post-Quantum Group-based Cryptography</b> , AIM workshop (invited, to come)	Pasadena CA, USA
02/23	<b>Young Geometric Group Theory XI</b> , Boundaries of relatively hyperbolic groups, Sofic groups	Münster, Germany
08/22	<b>Summer school in Post-quantum cryptography</b> , Isogeny based crypto., Lattice based crypto.	Budapest, Hungary
07/22	<b>A conference in honor of Joachim Rosenthal</b> , Cryptography, Coding theory	Zurich, Switzerland
06/22	<b>Hyperbolic groups and their generalisations</b> , part of IHP trimester program	Paris, France
06/21	<b>Young Geometric Group Theory X</b> , Actions on Trees and Cantor Sets, Helly graphs and groups	online
09/19	<b>Beyond Spectral Gaps</b> , Celebrating the Mathematics of Pierre Pansu	Oxford, UK
03/19	<b>ANR GAMME</b> , Groups, Actions, Metrics, Measures and Ergodic theory	St Etienne, France
01/19	<b>Groups and Geometries Master Class</b> , CAT(0) geometry, Lattices in Lie groups	Marseille, France
05/18	<b>ANR AGIRA</b> , IRS à Sète	St Etienne, France
05/18	<b>MathExp: Experimental Mathematics School</b> , Linear programming, Computer Algebra	St Flour, France
02/18	<b>Borel combinatorics and ergodic theory</b> , CIB conference	Lausanne, Switz.
10/17	<b>ANR GAMME</b> , Groups, Actions, Metrics, Measures and Ergodic theory	St Jean, France

## Teaching experience

---

### Teaching in Mathematics

GHENT UNIVERSITY

Bachelor thesis supervision: Bass-Serre theory with Lennert De Baecke  
(to come) Advanced Master course during the academic year 2023-2024.

Ghent, Belgium

2022 - 2024

### Teaching in Mathematics

UNIVERSITÉ PARIS-SACLAY

As main teacher: Computer algebra (L3), MEEF primary school teaching (M1)  
As teaching assistant: Calculus (L1), Differential Equations for biologists (L3), Linear algebra and analysis for engineers (L3)

Orsay, France

2017 - 2020

### Oral examinations

LYCÉE PIERRE DE COUBERTIN (MEAUX); INSTITUT BOSSUET, UNIVERSITÉ PARIS 7, LYCÉE SAINT-NICOLAS

Bachelor competitive exam training, including training examinations

Paris, France

2013 - 2018

## Referring

---

**PhD Committee** Harshit Jitendra Motwani (UGent, 2023)

**Journal** Paper review for Indiana University Mathematics Journal (2023)

## Computer skills

---

<b>Languages</b>	Python (good level), shell Bash (functional use), C (basic knowledge)
<b>Computer algebra</b>	Sagemath (very good mastery)
<b>Numerical analysis</b>	Scilab (basic knowledge)
<b>Version control</b>	Git (daily use)
<b>Edition</b>	$\LaTeX$ (very good mastery), Vim (daily use)

## Personal information

---

**Date of birth** July 1, 1992  
**Marital status** Married, three children  
**Nationality** French

## Miscellaneous

---

**Languages** French (native), English (fluent), Hebrew (notions)  
**Popularization** Active participation in math events for children: Math en Jean (2018), Journée de la Science (2018, 2019), UniMath (2023) workshop in a primary school at Massy (2019)  
**Youth movements** Management of a youth movement in Massy, France (2017-2020), of Scout groups in Paris and Caen, France (2014-2016)  
**Music** Guitar, drums, violin, and bass player.