Research statement

Corentin Le Coz

April 2022

Organization

Section 1 introduces my topic of research. Section 2 is devoted to an exposition of current applications of my work: prescription of high Poincaré profiles in §2.1, relations between isoperimetry and Poincaré profiles in §2.2, groups with logarithmic separation profile in §2.3, and cryptographic hash functions in §2.4.

1 My topic of research

My topics of research lie in the intersection of geometric group theory, metric geometry and graph theory. I've devoted most of my work in the study of the coarse geometry of finitely generated groups. To do so, I have developped applications of invariants called separation profile and Poincaré profiles, that has their roots in finite graph theory.

Separation profiles were introduced by Benjamini–Schramm–Timár [2,8] inspired by the celebrated Lipton–Tarjan theorem on planar graphs [17] and works from Miller–Teng–Thurston–Vavasis [21] for more general graphs.

Definition 1. Let G be an infnite graph. The separation profile of G is defined for every positive integer n by $\mathrm{sep}(n) = \sup_\Gamma |\Gamma| h(\Gamma)$, where the supremum is taken among subgraphs Γ conaining at most n vertices, and $h(\Gamma)$ denotes the Cheeger constant of the graph Γ.

The main interesting property of the aforementioned profiles is that they are monotonous under *coarse embeddings* (also known as uniform embeddings), meaning that if there is a coarse embedding of bounded degree graphs $G \to H$, then the profile of G is bounded above by that of H, up to constants.

Separation profile is thus a purely discrete tool. This profile has been generalized to analytic versions, involving p-Laplacians, by Hume-Mackay-Tessera [10], obtained by replacing Cheeger constants by p-Cheeger constants in the definition above. All this led me to study deeply Cheeger problems, analysis in finite graphs, and spectral graph theory.

2 Some applications of my work

2.1 Prescription of high separation profiles

When studying such invariants, it is important to know what values they can take, which led me to the study of the problem of the presciption of these profiles. It is clear from the definition that any Poincaré profiles is least constant and at most linear. It is then natural to ask what are the possible profiles within this range. I've done the first computation of almost linear profiles coming from amenable groups, using a family of groups constructed by Brieussel-Zheng in [6]. More precisely, I have proven the following statement:

Theorem 2. *[13] There exists two universal constants κ_1 and κ_2 such that the following is true. Let $\rho\colon \mathbb{R}_{\geq 1} \to \mathbb{R}_{\geq 1}$ be a non-decreasing function growing fastly enough[1]. Then, there exists a finitely generated elementary amenable group Δ of exponential growth and of asymptotic dimension one such that for any $p \in [1, \infty)$,*

$$\begin{aligned} & \Pi_{\Delta,p}(n) \leq \kappa_1 \frac{n}{\rho(\log n)} \quad \textit{for any } n, \\ \textit{and} \quad & \Pi_{\Delta,p}(n) \geq 4^{-p} \kappa_2 \frac{n}{\rho(\log n)} \quad \textit{for infinitely many } n\textit{'s}. \end{aligned}$$

The first application of this theorems concerns a theorem of Dranishinikov [7] stating that any graph with finite asymptotic dimension coarsely embeds into a finite profuct of trees. It is then natural to ask if these trees can be chosen having bounded degree. The theorem above and the computation of the separation profiles of products of trees [2] enables to prove that this is wrong in general:

Theorem 3. *[13] There exist bounded degree graphs of asymptotic dimension one that do not coarsely embed in any finite product of bounded degree trees.*

The second application that I will mention here concerns *distorsion* and *hyperfinite graphs.*

Bourgain showed in [4] that the p-distortion c_p of any finite graph is bounded by $O(\log n)$, where n denotes the number of vertices. It was proved to be optimal for families of expander graphs [16, 20]. The bound was improved by Rao [22] to $O(\sqrt{\log n})$ in the case of planar graphs. Since any family of planar graphs is hyperfinite [18], it is natural to ask if this bound is also valid for hyperfinite graphs. This question was raised to me by Gábor Pete. I have proven that this is wrong in general, by providing expicit examples of graphs with arbitrarily large distortion exponent (but strictly below log).

Theorem 4. *[13] For any $\epsilon \in (0,1)$, there exists a hyperfinite sequence of bounded degree graphs $(\Gamma_n)_{n\geq 0}$, such that for any $p \in [1, \infty)$ there is $K' = K'(p) > 0$ such that for any n,*

$$c_p(\Gamma_n) \geq K'(\log |\Gamma_n|)^{1-\epsilon}.$$

[1] I refer to the original paper for precise assumptions made on ρ

2.2 Isoperimetric profiles

In [15] written with Antoine Gournay, we give among other things comparison statements between separation profiles and isoperimetric profiles. This gave many new estimates on the separation profile of amenable Cayley graphs. One major application is the following theorem, stating that separation profile can detect virtual nilpotence among solvable groups.

Theorem 5. *[15] Let G be a finitely generated solvable group. If there exists $\epsilon \in (0,1)$ and $c > 0$ such that for any large enough integer n we have*

$$\mathrm{sep}_G(n) \leq cn^{1-\epsilon},$$

then G is virtually nilpotent.

Combining this with the computaton of profiles of cocompact lattices in hyperbolic spaces [2] and Bonk & Schamm's embedding result [3], it has the following corollary.

Corollary 6. *Let G be a finitely generated solvable group. If there exists a coarse embedding from G to a finitely generated hyperbolic group, then G is virtually nilpotent.*

This corollary was already obtained by Hume & Sisto [11], with a completely different proof.

The methods of [15] also yield to local results on the infinite percolation cluster of $\mathbb{Z}^d$, and more generally on a large class of graphs of polynomial growth, called polynomial graphs. Roughly speaking, a (d_1, d_2)-*polynomial graph* is a graph of volume growth bounded by n^{d_2} and of isoperimetric dimension at least d_1. We introduce a local variant of the separation profile in this context, namely the *local separation at v*, where v is a vertex of the graph:

$$\mathrm{sep}_G^v(n) := \sup_{F < B_G(v,r),\, |B_G(v,r)| \leq n} |F| \cdot h(F).$$

We show that $\frac{\mathrm{sep}_G^v(n)}{n}$ is bounded below by a function of the type $n^{-\alpha}$, for every vertices in the polynomial case, and for vertices that stay exponentially close to the origin in the $\mathbb{Z}^d$ percolation case:

Theorem 7. *[15] Let G be a (d_1, d_2)-polynomial graph. Then for any $\eta \in (0,1)$ there exists $c > 0$ such that for any vertex v and any integer n we have*

$$\mathrm{sep}^v(n) \geq cn^{(1-\eta)\frac{d_1^2(d_1-1)}{d_2^3}}.$$

The proof of this theorem is very algorithmic, I believe that this could lead to interesting applications, in particular in data analysis.

Theorem 8. *[15] Let $\mathcal{C}_\infty$ be a supercritical phase percolation cluster of $\mathbb{Z}^d$. Then for any $\varepsilon \in (0,1)$ there exists almost surely $c > 0$ such that for n large enough, if $\|v\|_\infty \leq \exp\left(n^{(1-\varepsilon)\frac{d}{d-1}}\right)$, then we have:*

$$\mathrm{sep}_{\mathcal{C}_\infty}^v(n) \geq cn^{\frac{d-1}{d}}.$$

The inclusion in $\mathbb{Z}^d$ shows that this lower bound is optimal.

2.3 Hyperbolic groups with logarithmic separation profiles

Every finitely presented group with separation profile bounded above by log, but not equivalent to it, have a constant separation profile. This implies that the group is virtually free (see [2,9]). Thus it is very natural to ask which groups have a logarithmic separation profile. With Nir Lazarovich, we showed [12]:

Theorem 9. *Let G be a hyperbolic group without 2-torsion. If $\mathrm{sep}_G(n) \preceq \log(n)$ then G can be inductively built from Fuchsian groups and free groups by amalgamations and HNN extensions over finite or virtually cyclic groups.*

This follows from Strong Accessibility by Louder-Touikan [19] and the following theorem.

Theorem 10. *Let G be a hyperbolic group with $\mathrm{sep}_G(n) \preceq \log(n)$, then G is Fuchsian or splits over finite or virtually cyclic subgroups.*

This theorem is showed using Bowditch's boundary criterion for splittings over cyclic groups [5]. Additionally, we show that the description of hyperbolic groups with logarithmic separation profiles is not complete, since there is no equivalence is Theorem 9. Indeed we provide in [12] an example of a surface amalgam with superlogarithmic separation profile.

2.4 Higher dimensional Tillich-Zémor hash functions

Recently, I have been interested in applications of geometric group theory to cryptography, more precisely to hash functions. A hash function is a map $\varphi : S \to H$, where all elements of H have the same "size", satisfying the two following properties:

- *preimage resistance:* given an element $h \in H$, it is computationally hard to find $s \in \varphi^{-1}(\{h\})$,
- *collision resistance:* it is computationally hard to find two distinct elements of S having the same image under φ.

The general idea of Tillich-Zémor [23] hash functions is the following. Starting at a base-point, the input to the hash function is used as a sequence of directions for a walk in a regular graph without backtracking, and the output of the hash function is the ending vertex of this walk.

With Christopher Battarbee, Ramón Flores, Thomas Koberda and Delaram Kahrobaei, we have built in [14] new Tillich-Zémor hash functions of this type. Using matrices $A, B \in \mathrm{SL}_n(\mathbb{F}_p)$ given by Goulnara Arzhantseva-Biswas in [1], we obtain graphs $G_{n,p}$ satisfying:

- the girth of $G_{n,p}$ is at least $c_n \log p$ for some constant c_n,

- the sequence $(G_{n,p})_p$ is an expander.

These two properties are highly desirable for preimage and collision resistance. To our knowledge, the only hash function proved to have these properties were broken. Here, the flexibility on the dimension enables to increase complexity of attacks.

References

[1] Goulnara Arzhantseva and Arindam Biswas. Large girth graphs with bounded diameter-by-girth ratio. *arXiv*, 03 2018.

[2] Itai Benjamini, Oded Schramm, and Ádám Timár. On the separation profile of infinite graphs. *Groups Geom. Dyn.*, 6(4):639–658, 2012.

[3] Mario Bonk and Oded Schramm. Embeddings of Gromov hyperbolic spaces. *Geom. Funct. Anal.*, 10(2):266–306, 2000.

[4] Jean Bourgain. On Lipschitz embedding of finite metric spaces in Hilbert space. *Israel J. Math.*, 52(1-2):46–52, 1985.

[5] Brian H. Bowditch. Cut points and canonical splittings of hyperbolic groups. *Acta mathematica*, 180(2):145–186, 1998.

[6] Jérémie Brieussel and Tianyi Zheng. Speed of random walks, isoperimetry and compression of finitely generated groups. *Ann. of Math. (2)*, 193(1):1–105, 2021.

[7] Alexander Nikolaevich Dranishnikov. On hypersphericity of manifolds with finite asymptotic dimension. *Trans. Amer. Math. Soc.*, 355(1):155–167, 2003.

[8] David Hume. A continuum of expanders. *Fund. Math.*, 238(2):143–152, 2017.

[9] David Hume and John M. Mackay. Poorly connected groups. *Proc. Amer. Math. Soc.*, 148(11):4653–4664, 2020.

[10] David Hume, John M. Mackay, and Romain Tessera. Poincaré profiles of groups and spaces. *Rev. Mat. Iberoam.*, 36(6):1835–1886, 2020.

[11] David Hume and Alessandro Sisto. Groups with no coarse embeddings into hyperbolic groups. *New York J. Math.*, 23:1657–1670, 2017.

[12] Nir Lazarovich and Corentin Le Coz. Hyperbolic groups with logarithmic separation profile, 2021.

[13] Corentin Le Coz. Poincaré profiles of lamplighter diagonal products, 2020.

[14] Corentin Le Coz, Christopher Battarbee, Ramón Flores, Thomas Koberda, and Delaram Kahrobaei. Higher dimensional platforms for Tillich-Zémor hash functions. *to appear on arXiv*, 2022.

[15] Corentin Le Coz and Antoine Gournay. Separation profiles, isoperimetry, growth and compression. *Preprint available from ArXiv, arXiv:1910.11733*, 2019.

[16] Nathan Linial, Eran London, and Yuri Rabinovich. The geometry of graphs and some of its algorithmic applications. *Combinatorica*, 15(2):215–245, 1995.

[17] Richard J. Lipton and Robert Endre Tarjan. A separator theorem for planar graphs. *SIAM J. Appl. Math.*, 36(2):177–189, 1979.

[18] Richard J. Lipton and Robert Endre Tarjan. Applications of a planar separator theorem. *SIAM J. Comput.*, 9(3):615–627, 1980.

[19] Larsen Louder and Nicholas Touikan. Strong accessibility for finitely presented groups. *Geometry & Topology*, 21(3):1805–1835, 2017.

[20] Jiří Matoušek. On embedding expanders into l_p spaces. *Israel J. Math.*, 102:189–197, 1997.

[21] Gary L. Miller, Shang-Hua Teng, William Thurston, and Stephen A. Vavasis. Separators for sphere-packings and nearest neighbor graphs. *J. ACM*, 44(1):1–29, 1997.

[22] Satish Rao. Small distortion and volume preserving embeddings for planar and Euclidean metrics. In *Proceedings of the Fifteenth Annual Symposium on Computational Geometry (Miami Beach, FL, 1999)*, pages 300–306. ACM, New York, 1999.

[23] Jean-Pierre Tillich and Gilles Zémor. Group-theoretic hash functions. In *Algebraic coding (Paris, 1993)*, volume 781 of *Lecture Notes in Comput. Sci.*, pages 90–110. Springer, Berlin, 1994.