AWS 2020: COMPUTATIONAL TOOLS FOR QUADRATIC CHABAUTY

JENNIFER BALAKRISHNAN

1. Course Outline

Given a smooth projective curve $X/\mathbf{Q}$, one aim of Kim's nonabelian Chabauty program [Kim09, Kim10a, Kim10b] is to determine $X(\mathbf{Q})$ algorithmically. This course will highlight the computational aspects of the *quadratic Chabauty* method [BD18, BD17, BDM+19], and in particular, describe algorithms used to compute the finite set of p-adic points $X(\mathbf{Q}_p)_2$ in certain cases where

$$r < g + \rho - 1,$$

where g is the genus of X, ρ is the Picard number of the Jacobian J, and $r = \operatorname{rk} J(\mathbf{Q})$. This course will be closely linked to Steffen Müller's course on the theoretical aspects of quadratic Chabauty. Here is a provisional outline of the lectures in this course.

Lecture I: The basic tools. Start by carrying out the linear algebra of explicit Chabauty–Coleman for curves over $\mathbf{Q}$, with Coleman integration as a black box. Describe how the Chabauty–Coleman diagram generalizes and motivate the presence of iterated Coleman integrals. Discuss Coleman integration [Col85, Bes12] and give preliminaries for explicit Coleman integration, starting with the p-adic point-counting algorithm of Kedlaya and Tuitman [Ked01, Ked07, Tui16, Tui17].

Lecture II: The basic tools, continued. Give algorithms for computing Coleman integrals of differentials of the first and second kind on curves [BBK10, BT17]. Describe algorithms to compute Coleman–Gross local p-adic heights [CG89, BB12], and in particular, Coleman integrals of 1-forms of the third kind on curves.

Lecture III: p-adic heights for quadratic Chabauty. Discuss the Nekovář p-adic height [Nek93] and our intended application. Show how universal properties [Kim09, Had11] lead us to computing the Hodge filtration and Frobenius structure. Reduce to linear algebra and solving p-adic differential equations.

Lecture IV: Examples. Apply the computation of the Nekovář height in a collection of examples to determine $X(\mathbf{Q})$. This could include bielliptic genus 2 curves, modular curves of genus 3 with real multiplication, and curves with few rational points. Discuss where the current frontier is and what remains to be done.

2. Projects

Below are some ideas for possible projects:

(1) *Coleman integration for curves over number fields and a Chabauty–Coleman solver.* The goals of this project would be to give an algorithm to compute Coleman integrals on curves over number fields, implement the algorithm, and use this to give a Chabauty-Coleman solver for curves over number fields that would take as input a genus g curve X defined over a number

Date: September 5, 2019.

field K with $r = \mathrm{rk}\, J(K) < g$, a prime $\mathfrak{p}$ of good reduction, and r generators of the Mordell–Weil group modulo torsion and output the set $X(K_{\mathfrak{p}})_1$.

Suggested reading: Coleman integration.

(2) *Quadratic Chabauty on modular curves* $X_0(N)^+$. Galbraith [Gal96, Gal99, Gal02] has constructed models for all modular curves $X_0(N)^+ = X_0(N)/w_N$ of genus ≤ 5 (with the exception of $N = 263$) and has conjectured that he has found all exceptional points on these curves. This project will use quadratic Chabauty to prove as much as possible about Galbraith's conjecture. Another goal is to investigate whether we can use p-adic Gross-Zagier to carry out quadratic Chabauty for $X_0(N)^+$, starting with the case of such curves of genus 2.

Suggested reading: Modular curves, p-adic heights, p-adic L-functions.

(3) *Quadratic Chabauty and Kim's conjecture.* When $X/\mathbf{Q}$ is a genus g curve with $r = \mathrm{rk}\, J(\mathbf{Q}) = g-1$, then typically the set of p-adic points $X(\mathbf{Q}_p)_1$ cut out by the Chabauty-Coleman method strictly contains $X(\mathbf{Q})$. In this project, we will first give an algorithm to compute the quadratic Chabauty set $X(\mathbf{Q}_p)_2$ under these hypotheses. Then we will investigate whether the quadratic Chabauty set, which satisfies

$$X(\mathbf{Q}) \subset X(\mathbf{Q}_p)_2 \subset X(\mathbf{Q}_p)_1 \subset X(\mathbf{Q}_p),$$

is equal to $X(\mathbf{Q})$. (See [Bia19] for the case of integral points on punctured elliptic curves.) If $X(\mathbf{Q}) \neq X(\mathbf{Q}_p)_2$, we would like to characterize the points in $X(\mathbf{Q}_p)_2 \setminus X(\mathbf{Q})$. This project could be carried out on a database of genus 2 and 3 curves [The19].

Suggested reading: Chabauty-Coleman method, p-adic heights.

For the computational part of Projects 1 and 3, we will use the computer algebra system `Magma`. For Project 2, `Magma` would be useful, but restricting to the case of hyperelliptic curves would also be very interesting (and likely more tractable, from the point of view of determining Mordell–Weil ranks unconditionally), and in this case, we could use `SageMath`.

References

[BB12] J. S. Balakrishnan and A. Besser. Computing local p-adic height pairings on hyperelliptic curves. *IMRN*, 2012(11):2405–2444, 2012. ↑1.

[BBK10] J. S. Balakrishnan, R. W. Bradshaw, and K. Kedlaya. Explicit Coleman integration for hyperelliptic curves. In *Algorithmic number theory*, volume 6197 of *Lecture Notes in Comput. Sci.*, pages 16–31. Springer, Berlin, 2010. ↑1.

[BD17] Jennifer S Balakrishnan and Netan Dogra. Quadratic Chabauty and rational points II: Generalised height functions on Selmer varieties. *arXiv preprint arXiv:1705.00401*, 2017. ↑1.

[BD18] Jennifer S. Balakrishnan and Netan Dogra. Quadratic Chabauty and rational points I: p-adic heights. *Duke Math. J.*, 167(11):1981–2038, 2018. ↑1.

[BDM$^+$19] J. S. Balakrishnan, N. Dogra, J. S. Müller, J. Tuitman, and J. Vonk. Explicit Chabauty–Kim for the split Cartan modular curve of level 13. *Ann. of Math. (2)*, 189(3):885–944, 2019. ↑1.

[Bes12] A. Besser. Heidelberg lectures on Coleman integration. In Jakob Stix, editor, *The Arithmetic of Fundamental Groups*, volume 2 of *Contributions in Mathematical and Computational Sciences*, pages 3–52. Springer Berlin Heidelberg, 2012. ↑1.

[Bia19] Francesca Bianchi. Quadratic Chabauty for (bi)elliptic curves and Kim's conjecture. arXiv:1904.04622, 2019. ↑3.

[BT17] Jennifer S. Balakrishnan and Jan Tuitman. Explicit Coleman integration for curves. *Arxiv preprint*, 2017. ↑1.

[CG89] Robert F. Coleman and Benedict H. Gross. p-adic heights on curves. In *Algebraic number theory*, volume 17 of *Adv. Stud. Pure Math.*, pages 73–81. Academic Press, Boston, MA, 1989. ↑1.

[Col85] R. Coleman. Torsion points on curves and p-adic abelian integrals. *Annals of Math.*, 121:111–168, 1985. ↑1.

[Gal96] S. D. Galbraith. Equations for modular curves. *Oxford DPhil thesis*, 1996. ↑2.

[Gal99] Steven D. Galbraith. Rational points on $X_0^+(p)$. *Experiment. Math.*, 8(4):311–318, 1999. ↑2.

[Gal02] Steven D. Galbraith. Rational points on $X_0^+(N)$ and quadratic $\mathbb{Q}$-curves. *J. Théor. Nombres Bordeaux*, 14(1):205–219, 2002. ↑2.

[Had11] M. Hadian. Motivic fundamental groups and integral points. *Duke Math. J.*, 160(3):503–565, 2011. ↑1.

[Ked01] K. S. Kedlaya. Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. *J. Ramanujan Math. Soc.*, 16:323–338, 2001. erratum *ibid.* **18** (2003), 417–418. ↑1.

[Ked07] K. Kedlaya. *p*-Adic cohomology: from theory to practice. *Arizona Winter School Notes*, 2007. ↑1.

[Kim09] M. Kim. The unipotent Albanese map and Selmer varieties for curves. *Publ. RIMS*, 45:89–133, 2009. ↑1.

[Kim10a] M. Kim. Massey products for elliptic curves of rank 1. *J. Amer. Math. Soc.*, 23(3):725–747, 2010. ↑1.

[Kim10b] M. Kim. *p*-Adic L-functions and Selmer varieties associated to elliptic curves with complex multiplication. *Ann. of Math. (2)*, 172(1):751–759, 2010. ↑1.

[Nek93] J. Nekovar. On *p*-adic height pairings. In *Séminaire de Théorie des Nombres, Paris 1990-1991*, pages 127–202. Birkhäuser, 1993. ↑1.

[The19] The LMFDB Collaboration. The L-functions and Modular Forms Database. http://www.lmfdb.org, 2019. [Online; accessed 1 July 2019]. ↑3.

[Tui16] Jan Tuitman. Counting points on curves using a map to $\mathbf{P}^1$. *Math. Comp.*, 85(298):961–981, 2016. ↑1.

[Tui17] Jan Tuitman. Counting points on curves using a map to $\mathbf{P}^1$, II. *Finite Fields Appl.*, 45:301–322, 2017. ↑1.

E-mail address: jbala@bu.edu